

CYBER

FORENSICS

A PRACTICAL REPORT

ON

CYBER FORENSICS

SUBMITTED BY

Mr. BHAVISHAY MANKANI

Roll No: 22009

UNDER THE GUIDANCE OF

PROF. ANSHIKA GAUTAM

Submitted in fulfilment of the requirements for qualifying
MSc. IT Part II Semester - IV Examination 2023-2024

University of Mumbai

Department of Information Technology

R.D. & S.H National College of Arts, Commerce & S.W.A.
Science College Bandra (West), Mumbai – 400 050



R. D. & S. H. National & S. W. A. Science College

Bandra (W), Mumbai - 400050

**Department of Information Technology
M.Sc. (IT – SEMESTER IV)**

Certificate

This is to certify that Cyber Forensics Practical's performed at R.D & S.H National & S.W.A. Science College by Mr. Bhavishay Mankani holding Seat No. _____ studying Master of Science in Information Technology Semester – IV has been satisfactorily completed as prescribed by the University of Mumbai, during the year 2023 – 2024

Subject In-Charge

Coordinator In-Charge

External Examiner

College Stamp

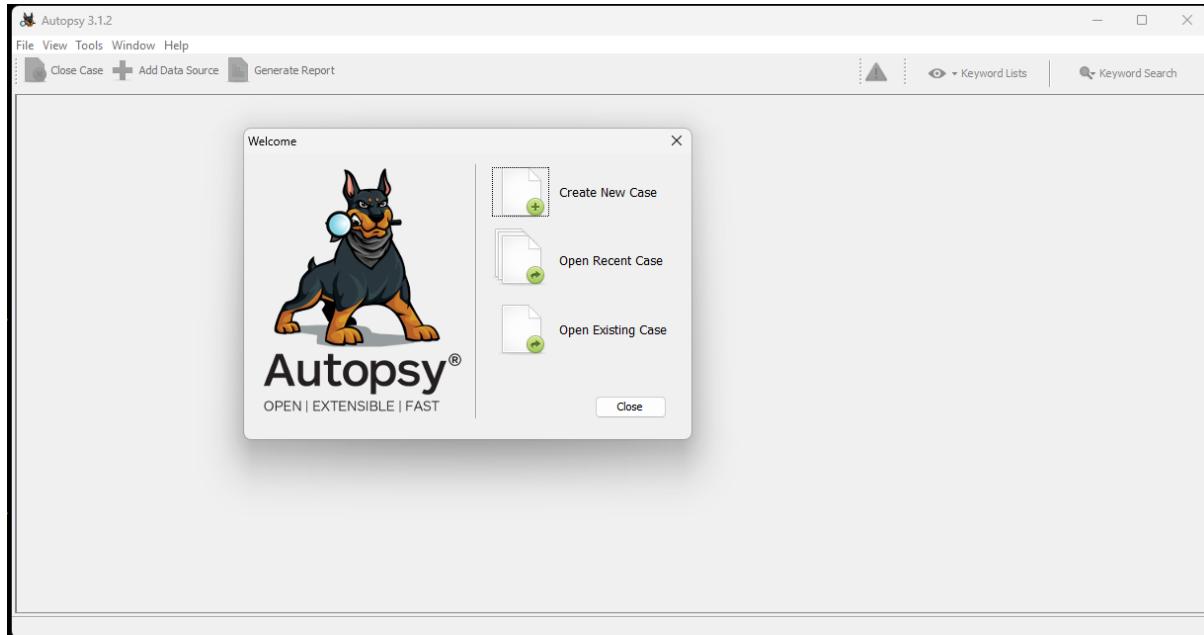
INDEX

Sr. No	Date	Practical	Page No.	Sign
1	24/04/2024	File system Analysis using The Sleuth kit.	1	
2	01/05/2024	Using Forensic Toolkit (FTK) & Writing report using FTK (Access Data FTK)	11	
3	15/05/2024	Understanding & working with the process of taking a drive image using Access Data's FTK Imager tool.	36	
4	22/05/2024	Using Wireshark Tool.	46	
5	29/05/2024	Using Data Acquisition Tools [ProDiscover Pro]	54	
6	05/06/2024	Using Steganography Tools [S-Tools]	62	
7	12/06/2024	Performing Sniffing and Password Cracking Using Cain and Abel.	73	

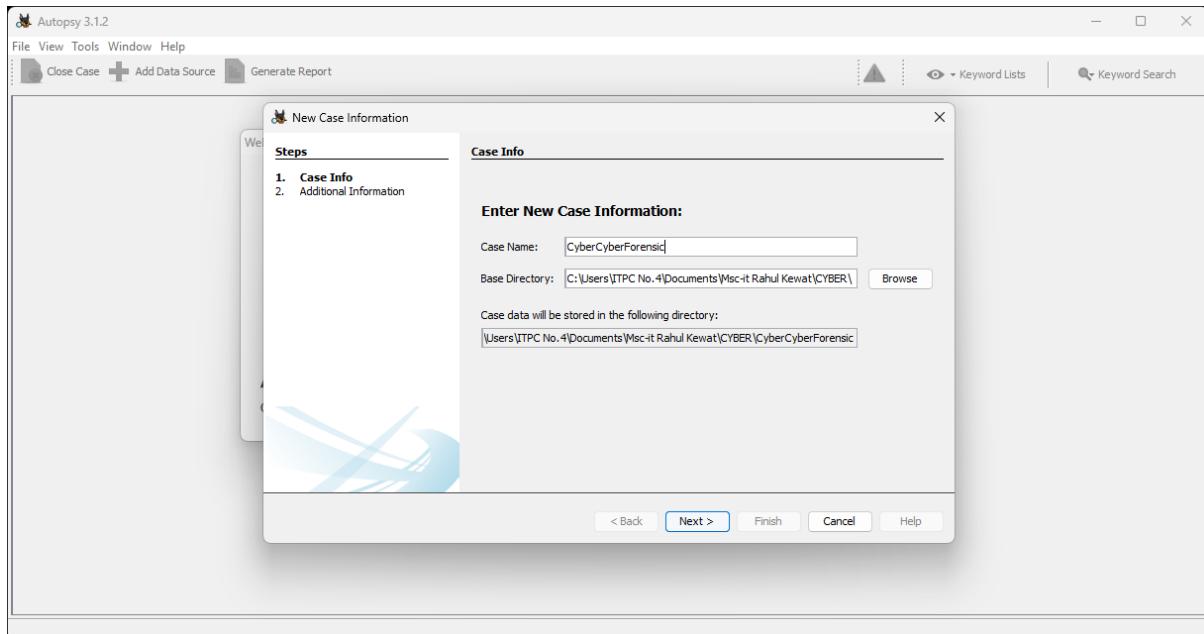
Practical: 1

Aim: File system Analysis using The Sleuth kit.

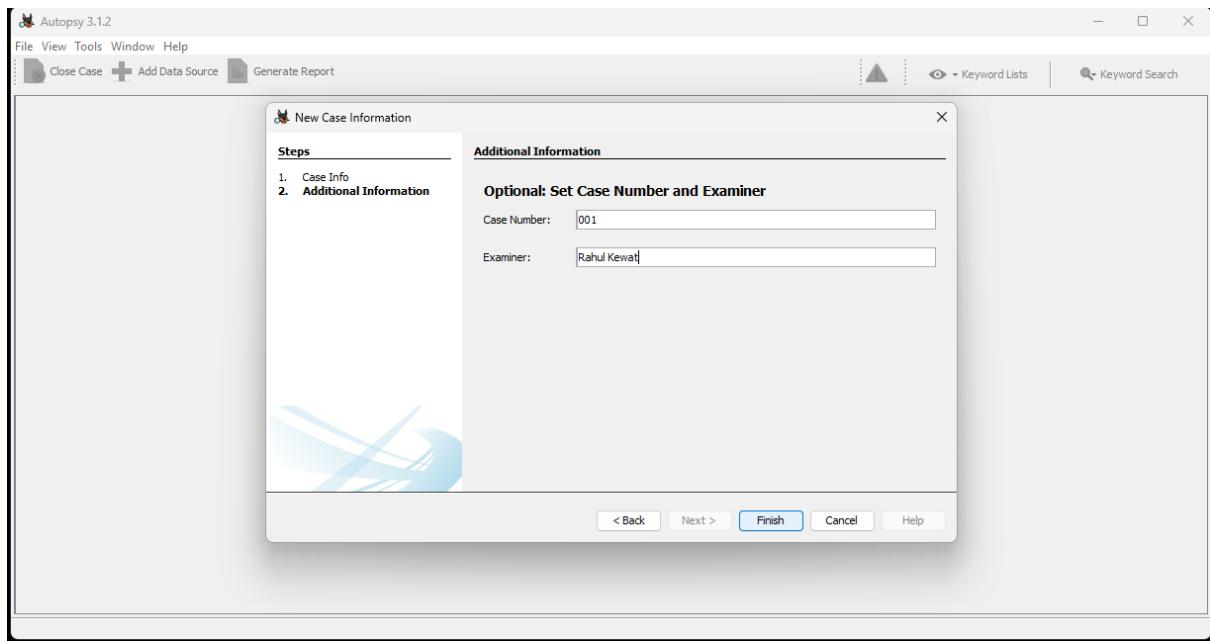
Writeup:

Step 1: Open Autopsy 3.12 and Click on Create New Case

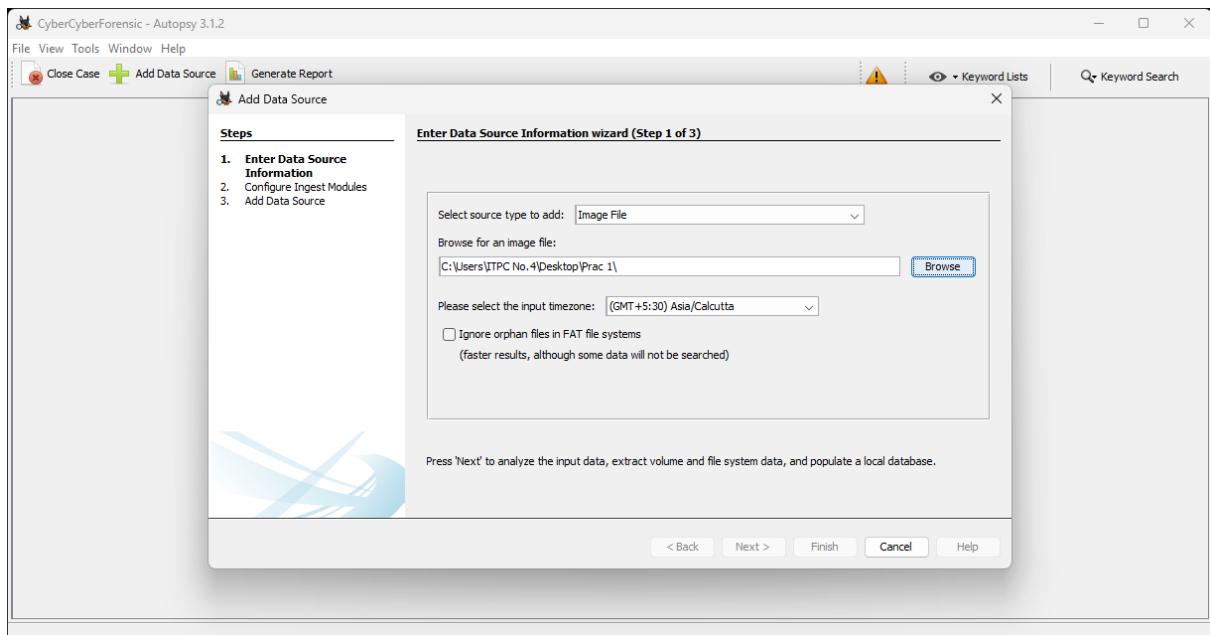
Step 2: Within Enter New Case Information Type Case Name (Here it is CyberForensic) and Click on Browse and Select Base Directory and Click on Next



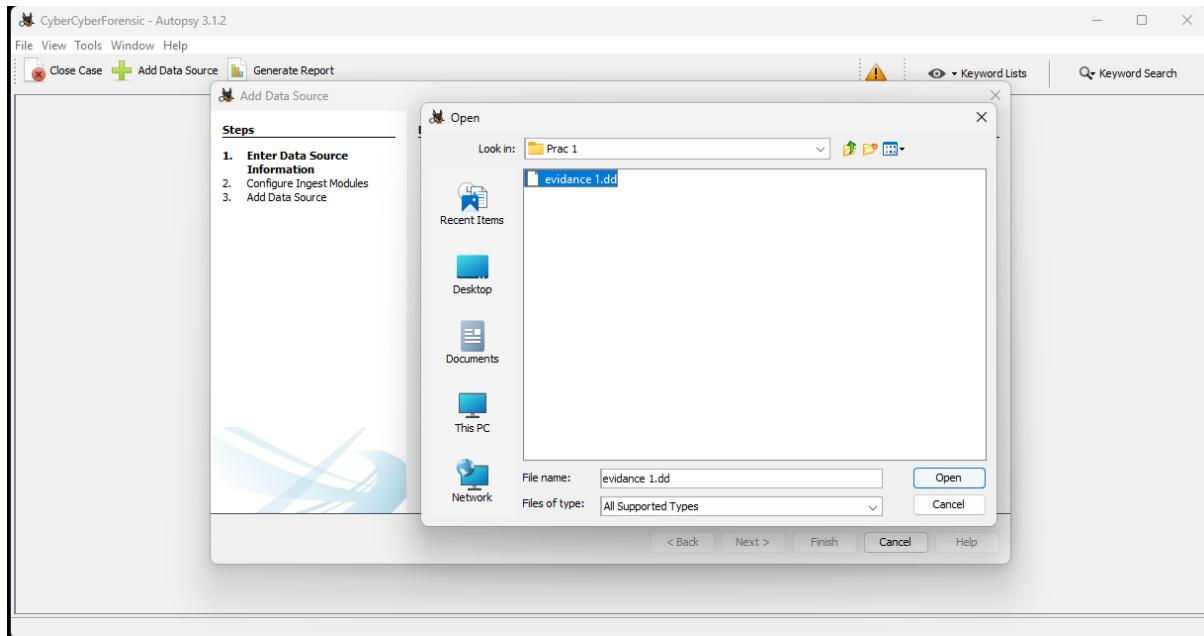
Step 3: Within Additional Information Set Case Number and Examiner Here it is **Case Number 001** And **Examiner Name Rahul Kewat** and **Click on Finish**



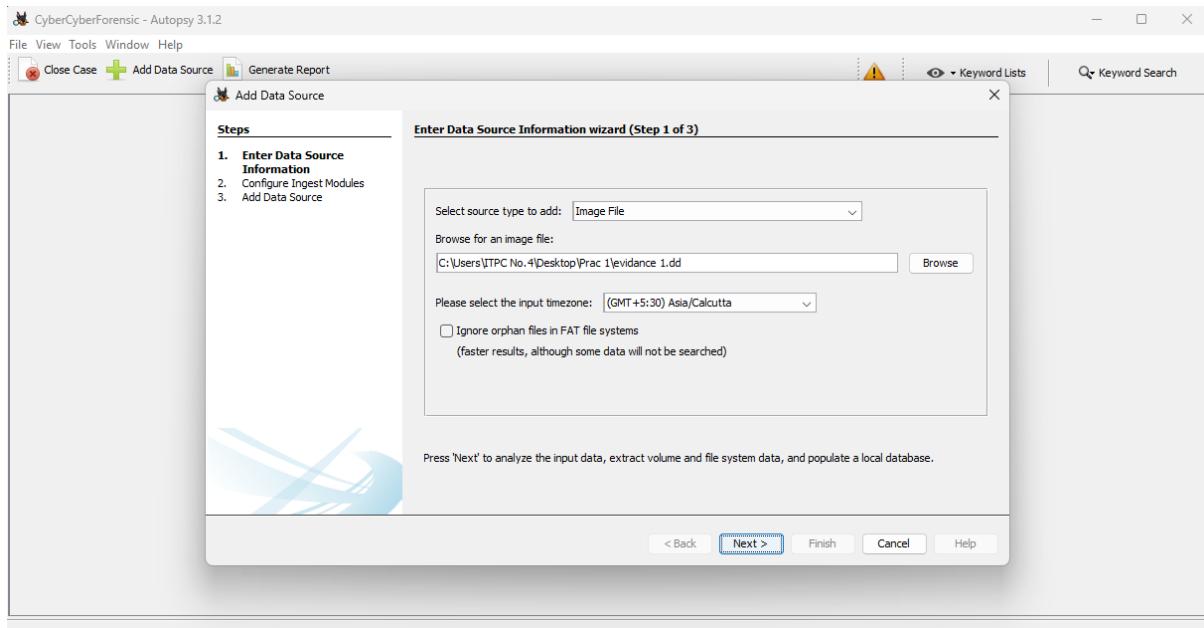
Step 4: The next step in the investigation will be to add an image file to the case. Within **Enter Data Source Information** Select source type to add: Here we select **Image File** and **Click on Browse**

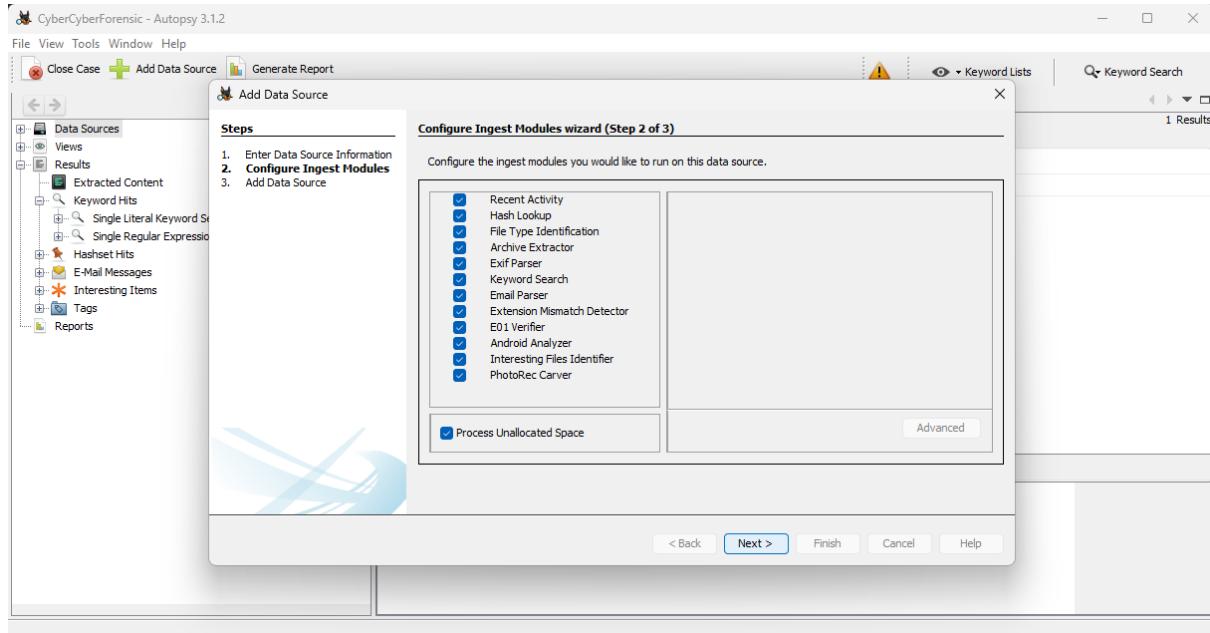
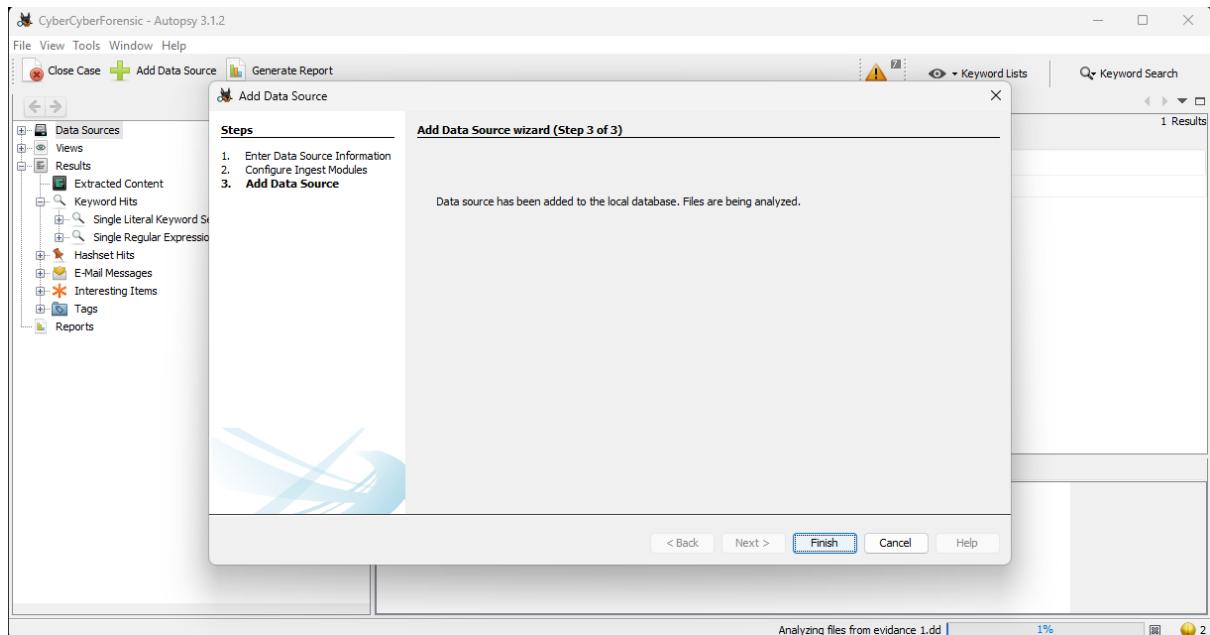


- After Click on Browse Select evidence1.dd Click on Open

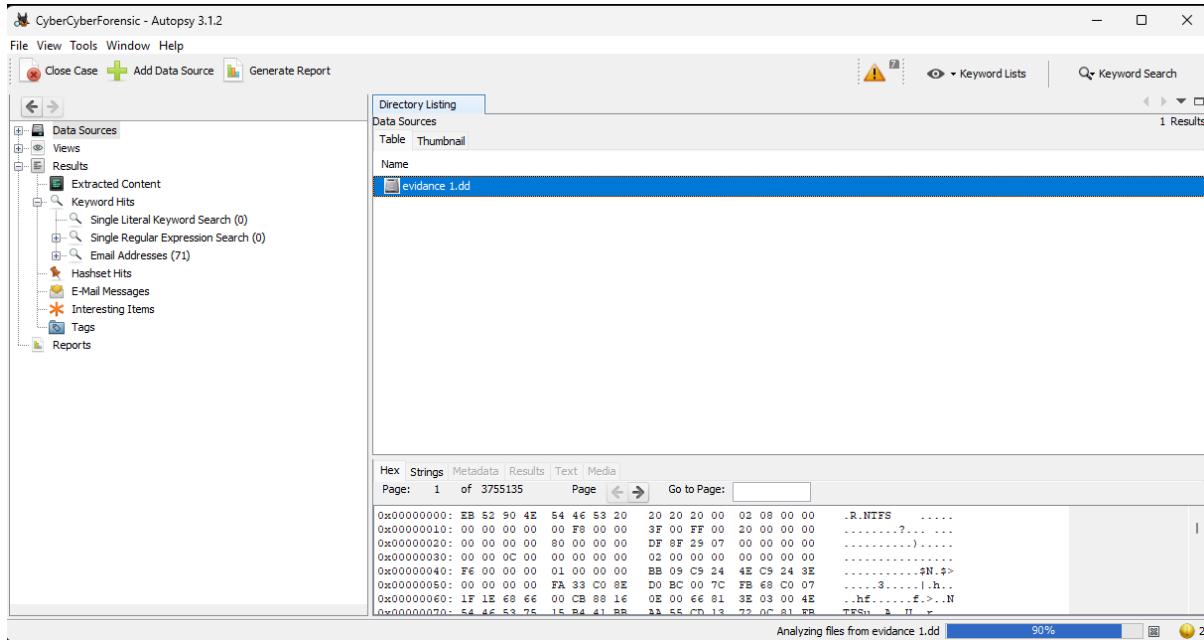


- Click on Next

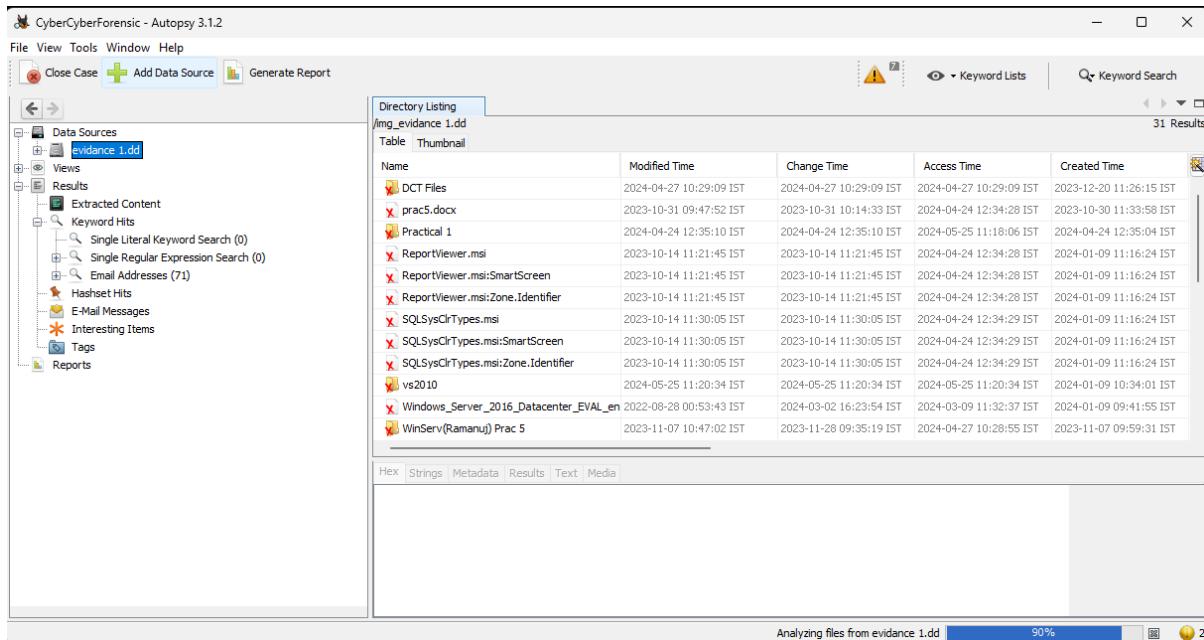


Step 5: In configuration Ingest Modules Keep Default Setting and Click on Next**Step 6: Click on Finish**

Step 7: It Analyzing the Files From evidence 1.dd

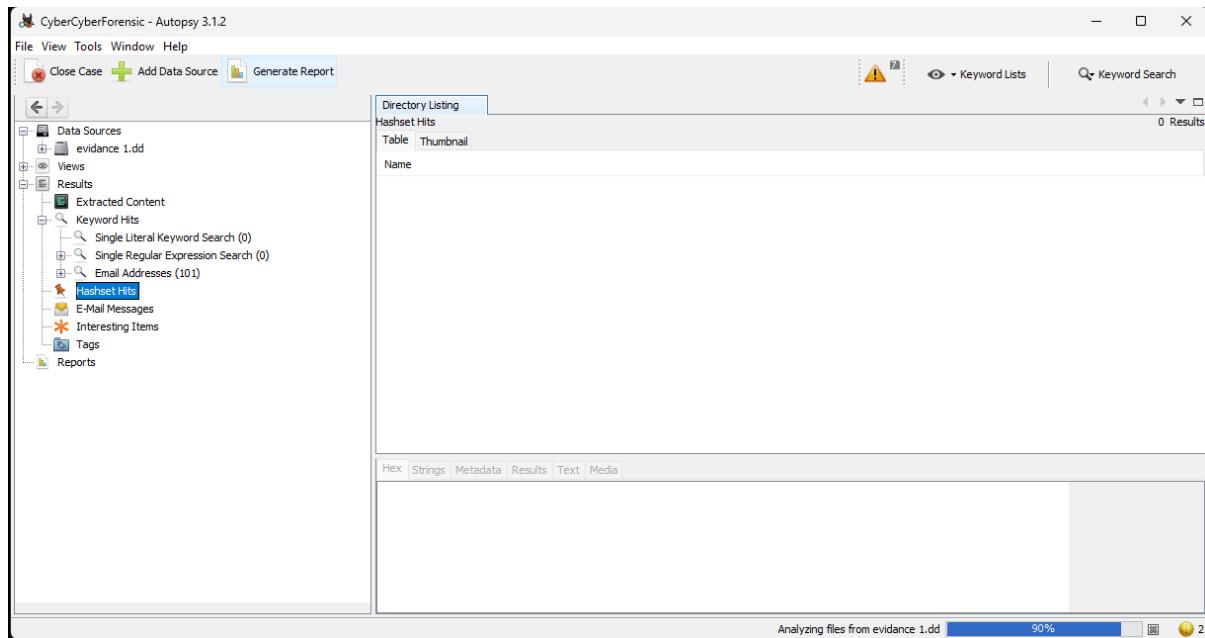


Step 8: Expand the Data Source there is one Hard Drive under Data Source Called evidence 1.dd by selecting evidence 1.dd we can see file structure or files in main view in the main view we can see the file name special attribute modified time change time access time.

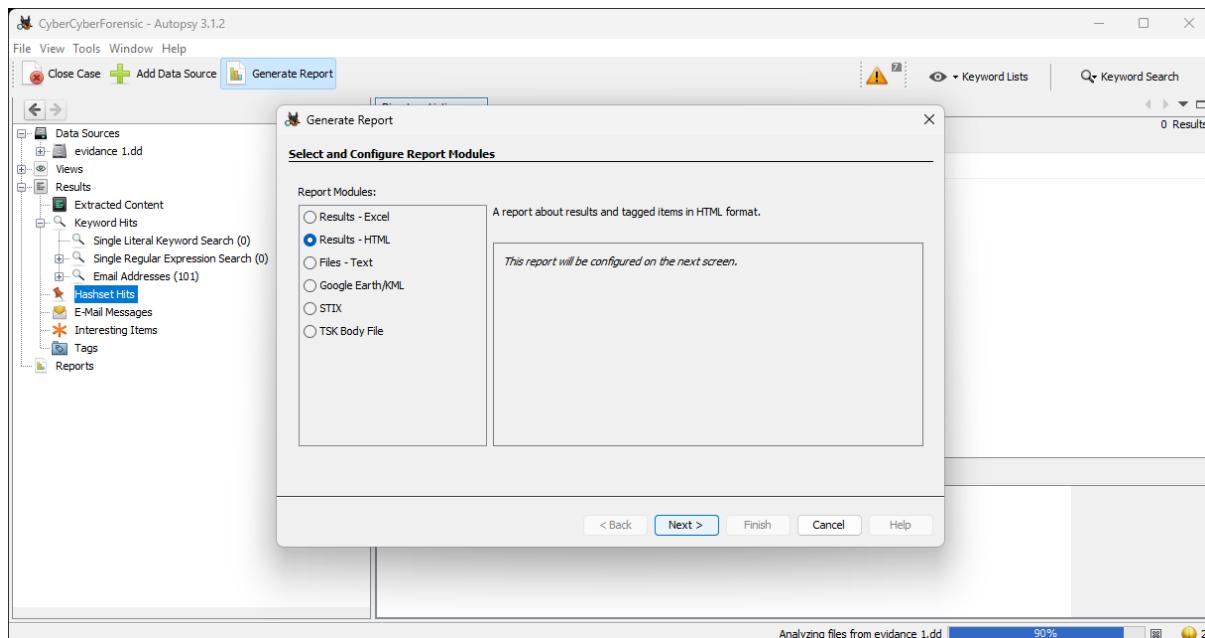


Step 9: After the image is indexed the tree will be populated by the file system, extracted content, keyword searches, and the hash list (if any were used). the investigator should generate a report. This will allow the investigator to have an idea of what type of information is available and what to expect. The report can be generated in three formats: Excel, XML, and HTML.

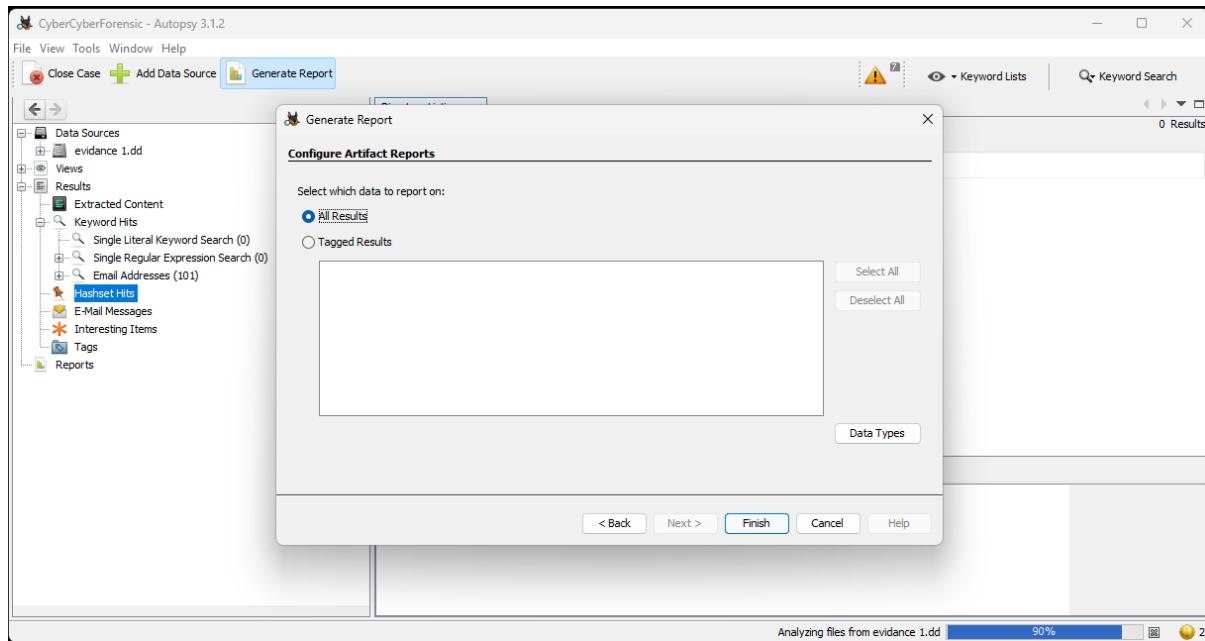
- Click on Generate Report



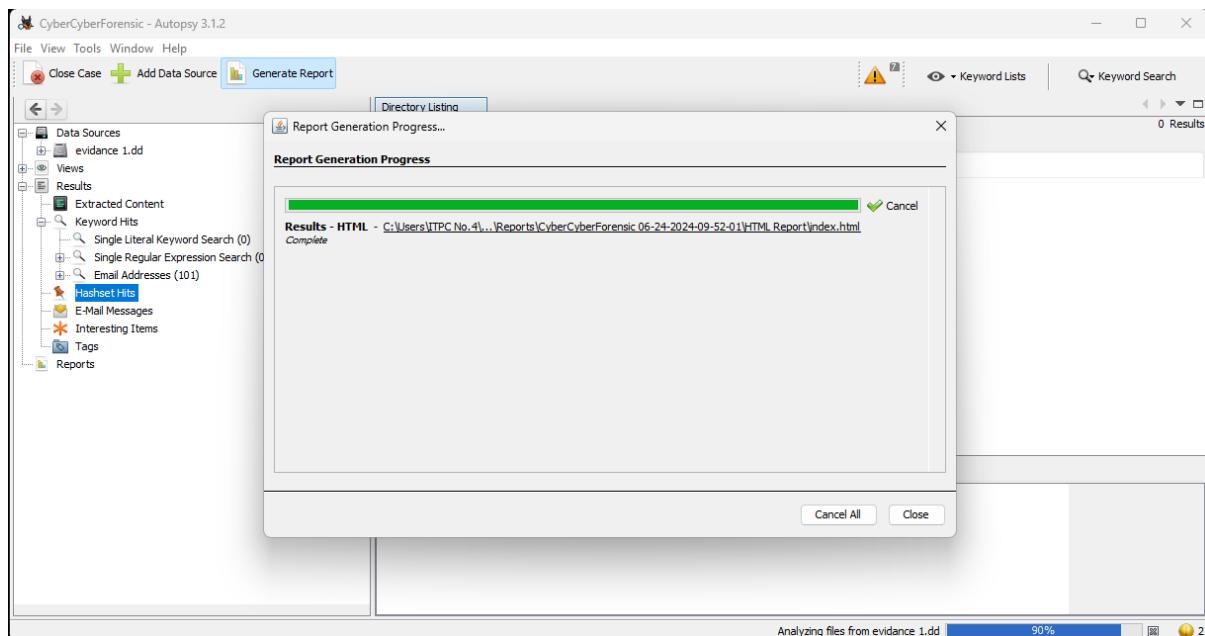
- Select Result-HTML and Click on Next



- Select All Results and Click on Finish



- Report Generation in Progress After Completion Click on Given link to view the Report



- Report Generated

The screenshot shows the Autopsy Forensic Report interface. On the left, there is a 'Report Navigation' sidebar with links to Case Summary, Keyword Hits (101), Tagged Files (0), Tagged Results (0), and Thumbnails (0). The main area is titled 'Autopsy Forensic Report' and displays a warning: 'Warning, this report was run before ingest services completed!' Below this, it shows the case details: Case: CyberCyberForensic, Case Number: 001, Examiner: Rahul Kewat, and Number of Images: 1. Under 'Image Information:', it lists 'evidence 1.dd' with Timezone: Asia/Calcutta and Path: C:\Users\ITPC No.4\Desktop\Prac 1\evidence 1.dd. A small image of a Doberman Pinscher is displayed.

Step 10: View image detail

- Right-Click on evidence 1.dd and Select image Details

The screenshot shows the CyberCyberForensic - Autopsy 3.1.2 interface. The left sidebar shows 'Data Sources' with 'evidence 1.dd' selected. A context menu is open over 'evidence 1.dd' with options like 'Extract Unallocated Space to Single Files', 'Open File Search by Attributes', 'Run Ingest Modules', and 'Collapse All'. The main pane displays a table titled 'Image Details' with columns: Name, Modified Time, Change Time, Access Time, and Created Time. The table lists various files from the evidence, such as DCT Files, prac5.docx, Practical 1, ReportViewer.msi, ReportViewer.msi:SmartScreen, ReportViewer.msi:Zone.Identifier, SQLSysClrTypes.msi, SQLSysClrTypes.msi:SmartScreen, SQLSysClrTypes.msi:Zone.Identifier, vs2010, Windows_Server_2016_Datacenter_EVAL_en, and WinServ(Ramanuj) Prac 5. At the bottom, a progress bar indicates 'Analyzing files from evidence 1.dd' at 90% completion.

- Here we can see Image Information

Image Details

Image Information

Name:	evidence 1.dd						
Type:	Raw Single						
Sector Size:	512						
Total Size:	61524131328						
Hash Value:	61524131328						
Modified Time	2024-04-27 10:29:09 IST	Change Time	2024-04-27 10:29:09 IST	Access Time	2024-04-27 10:29:09 IST	Created Time	2023-12-20 11:26:15 IST
	2023-10-31 09:47:52 IST	2023-10-31 10:14:33 IST	2024-04-24 12:34:28 IST	2023-10-30 11:33:58 IST			
	2024-04-24 12:35:10 IST	2024-04-24 12:35:10 IST	2024-05-25 11:18:06 IST	2024-04-24 12:35:04 IST			
	2023-10-14 11:21:45 IST	2023-10-14 11:21:45 IST	2024-04-24 12:34:28 IST	2024-01-09 11:16:24 IST			
	2023-10-14 11:21:45 IST	2023-10-14 11:21:45 IST	2024-04-24 12:34:28 IST	2024-01-09 11:16:24 IST			
	2023-10-14 11:21:45 IST	2023-10-14 11:21:45 IST	2024-04-24 12:34:28 IST	2024-01-09 11:16:24 IST			
	2023-10-14 11:30:05 IST	2023-10-14 11:30:05 IST	2024-04-24 12:34:29 IST	2024-01-09 11:16:24 IST			
	2023-10-14 11:30:05 IST	2023-10-14 11:30:05 IST	2024-04-24 12:34:29 IST	2024-01-09 11:16:24 IST			
	2024-05-25 11:20:34 IST	2024-05-25 11:20:34 IST	2024-05-25 11:20:34 IST	2024-01-09 10:34:01 IST			
	2022-08-28 00:53:43 IST	2024-03-02 16:23:54 IST	2024-03-09 11:32:37 IST	2024-01-09 09:41:55 IST			
	2023-11-07 10:47:02 IST	2023-11-28 09:35:19 IST	2024-04-27 10:28:55 IST	2023-11-07 09:59:31 IST			

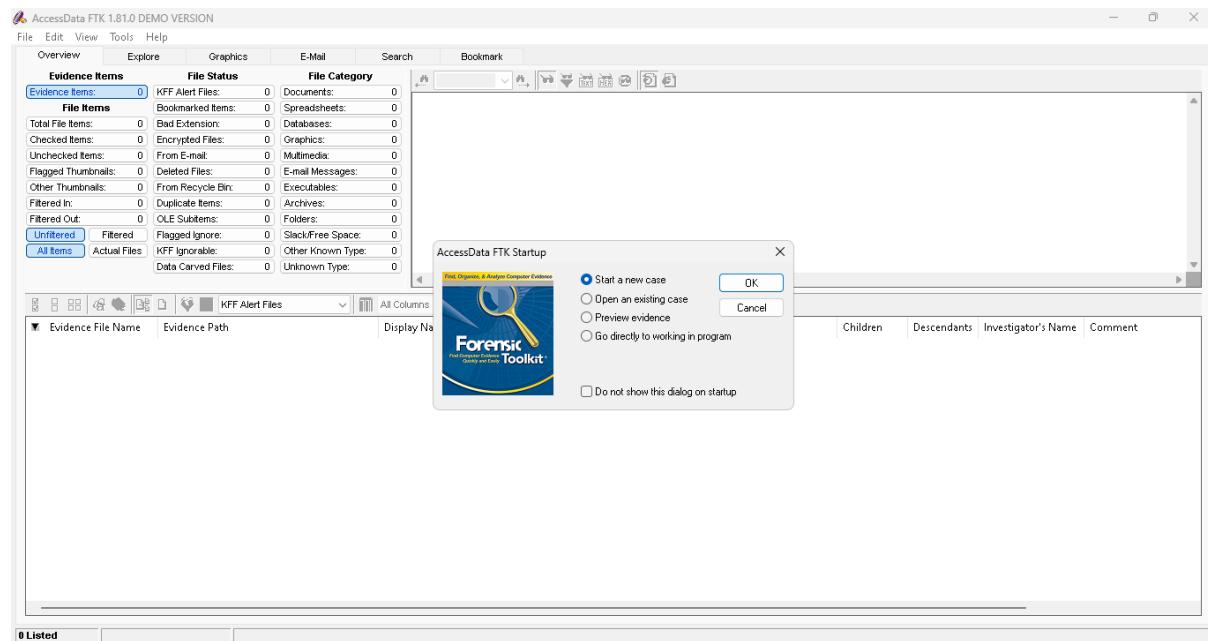
Analyzing files from evidence 1.dd 90% (1 more...) 2

Practical: 2

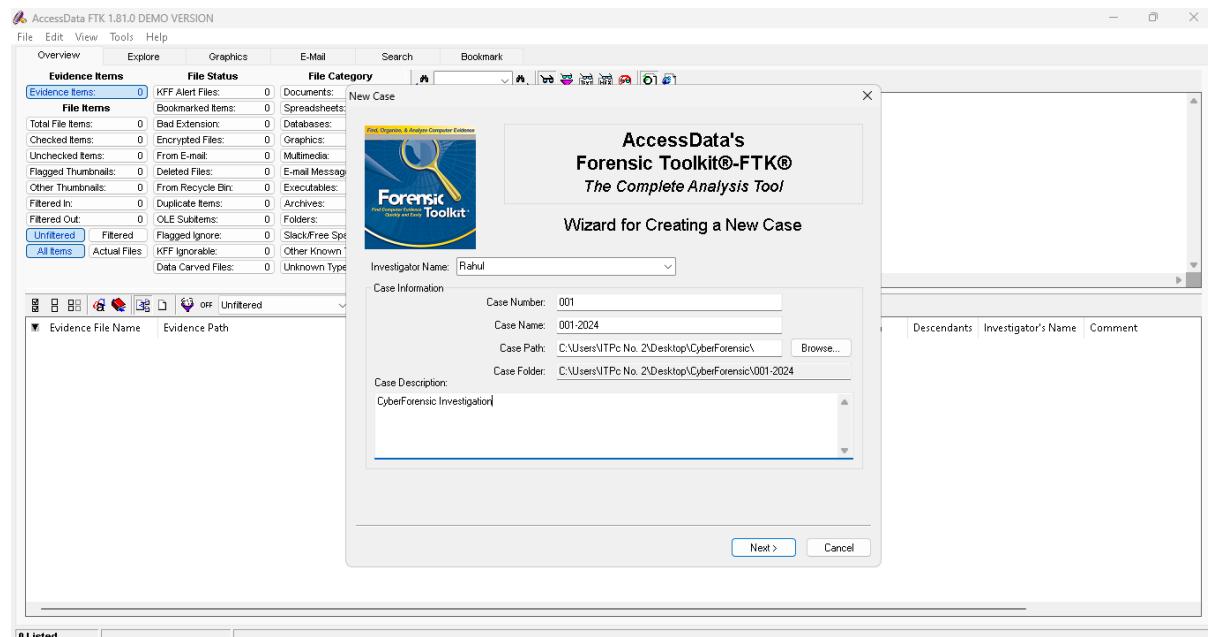
Aim: Using Forensic Toolkit (FTK) & Writing report using FTK (AccessData FTK).

Writeup:

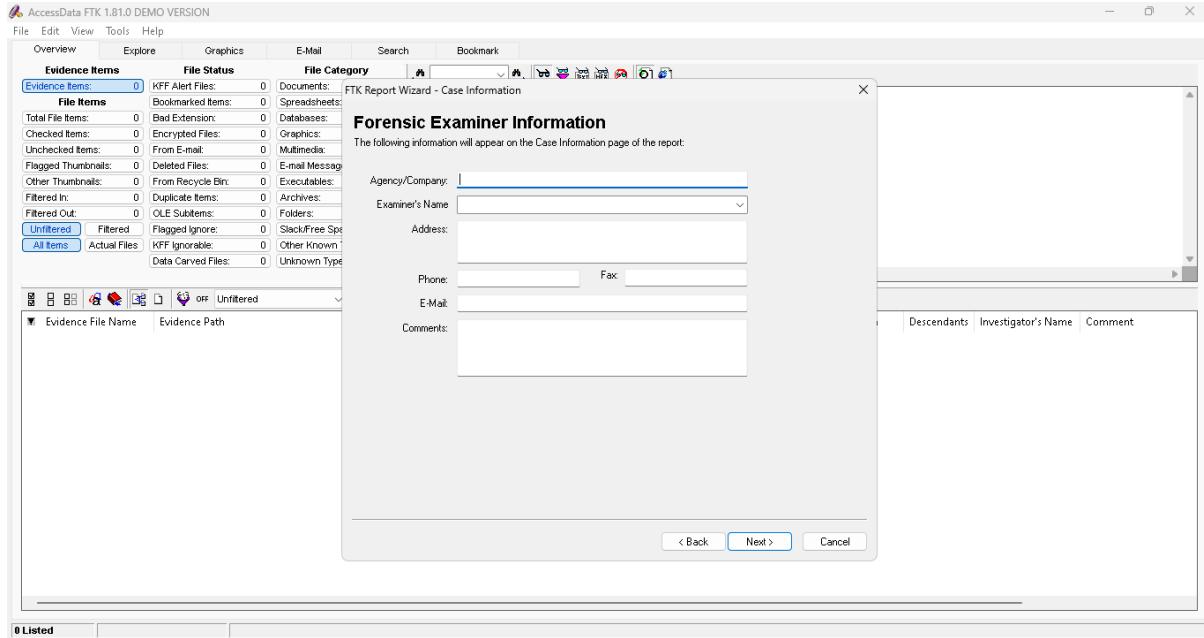
Step 1: Open AccessData FTK 1.81.0 DEMO VERSION and Click on Start a new case and Click on OK



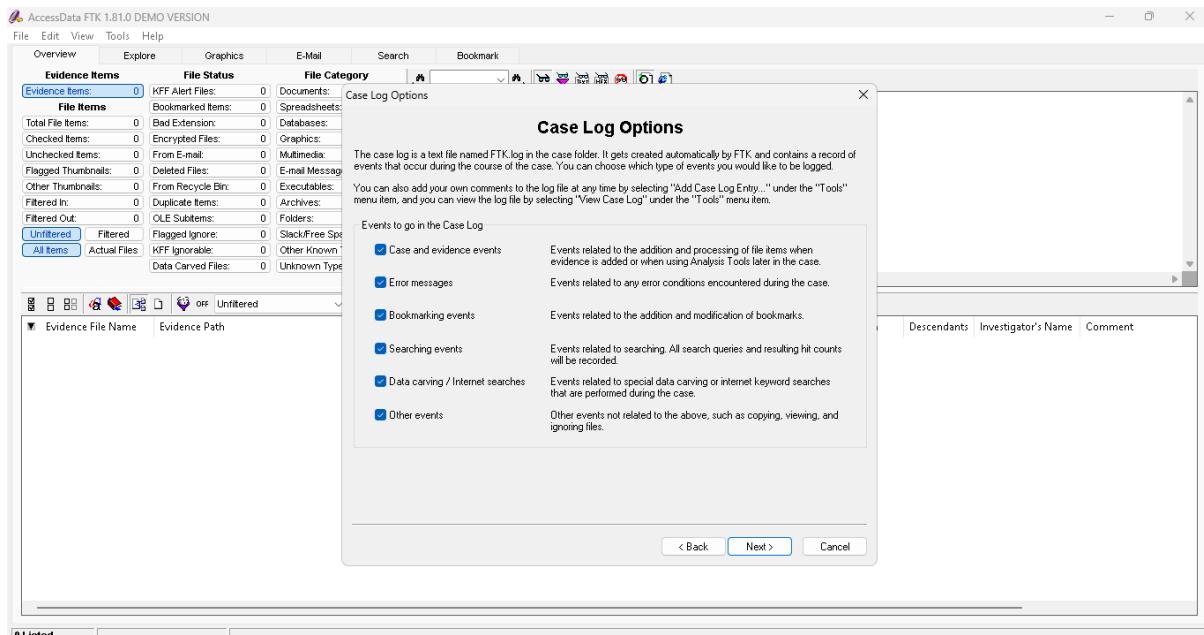
Step 2: Type Investigator Name and Case Number, Case Name and Set the Case Path and Click on Next



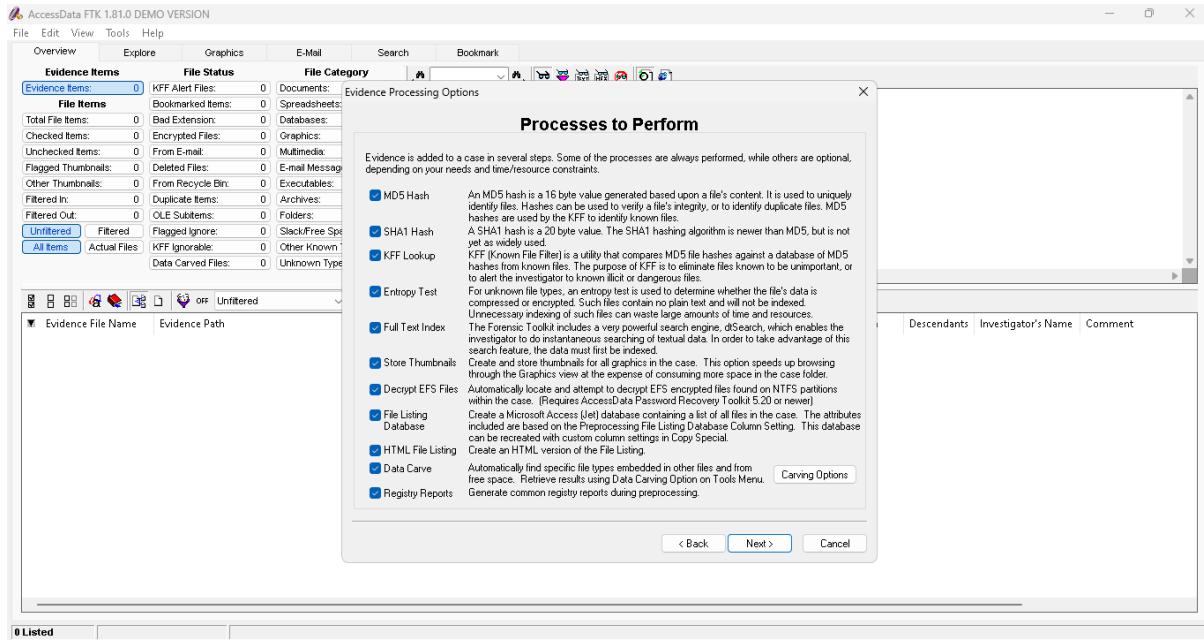
Step 3: Keep Default Setting and Click on Next



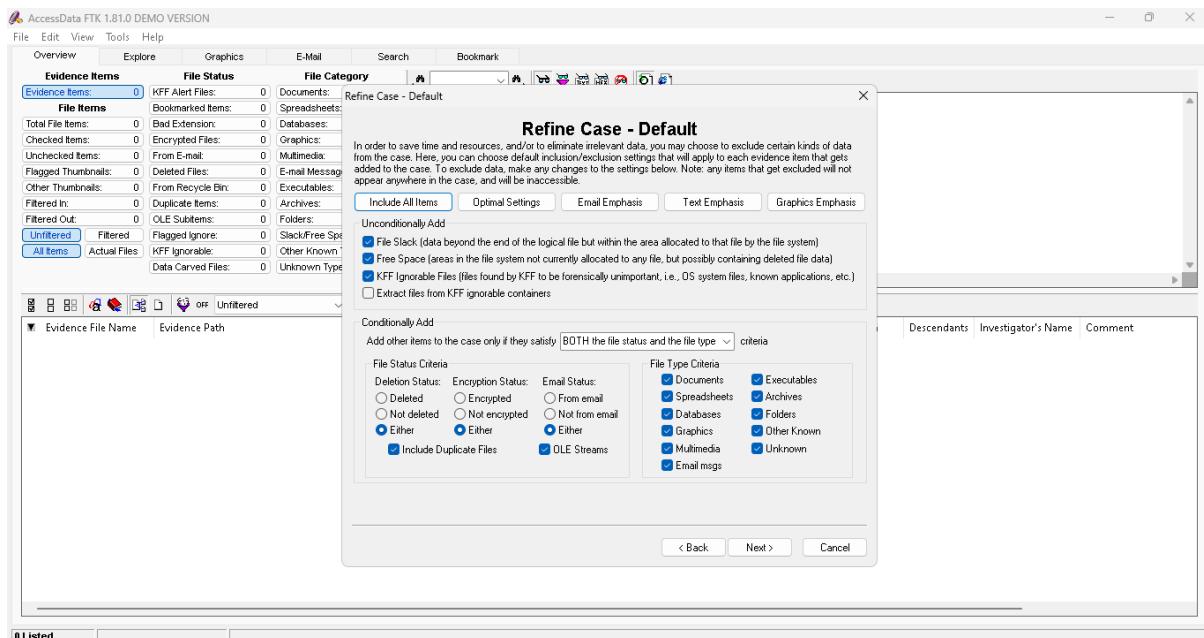
Step 4: Keep Default Setting and Click on Next



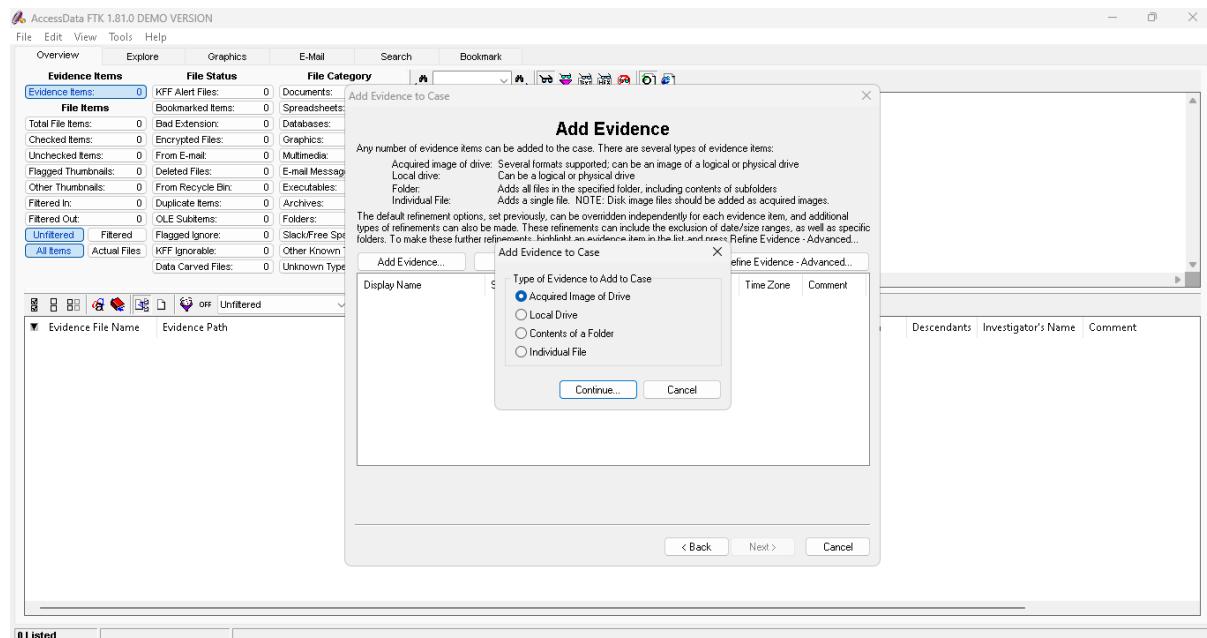
Step 5: Select Data Carve and Registry Report and Click on Next



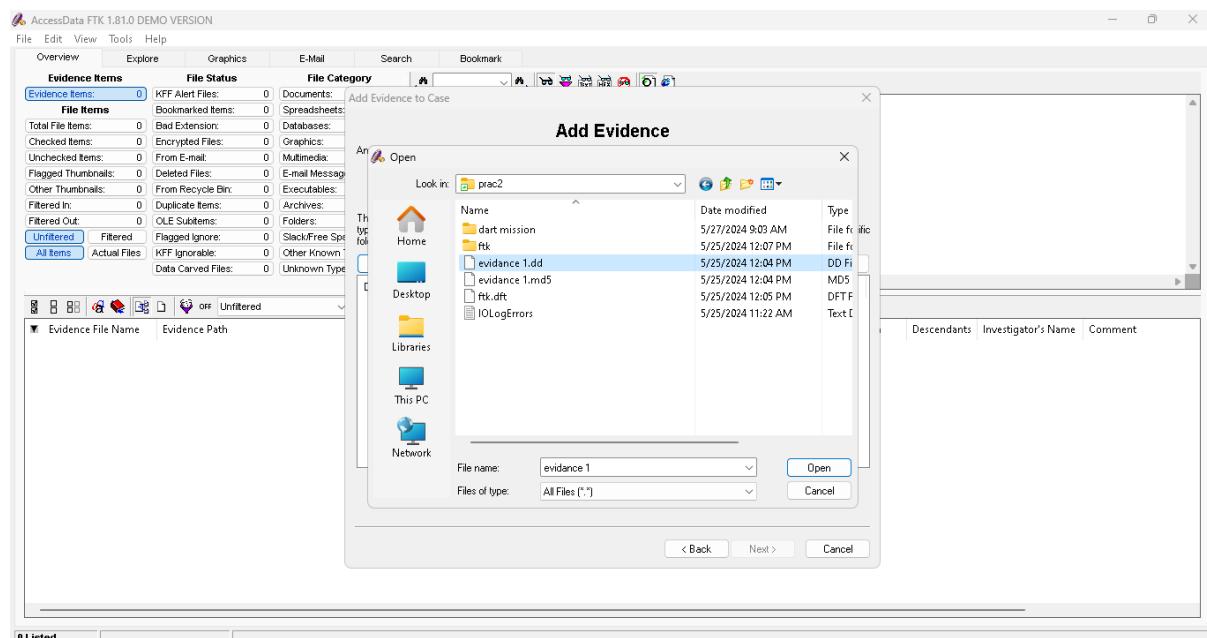
Step 6: Keep Default Setting and Click on Next



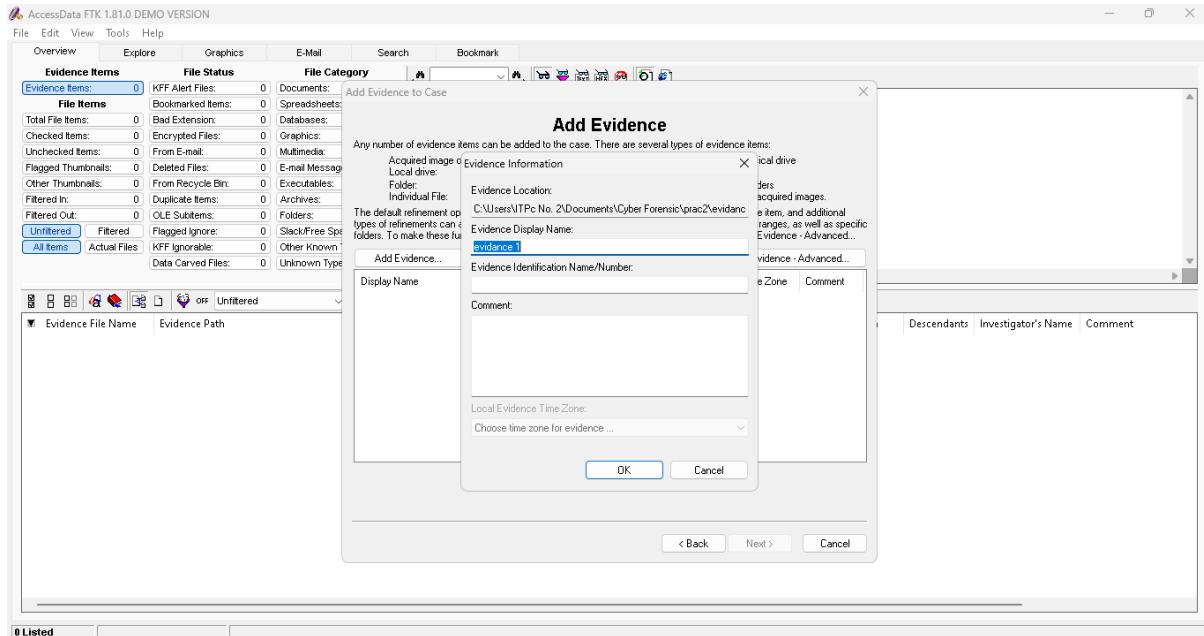
Step 7: Click on Add Evidence Within Type of Evidence to Add to Case Select Acquired Image of Drive and Click on Continue



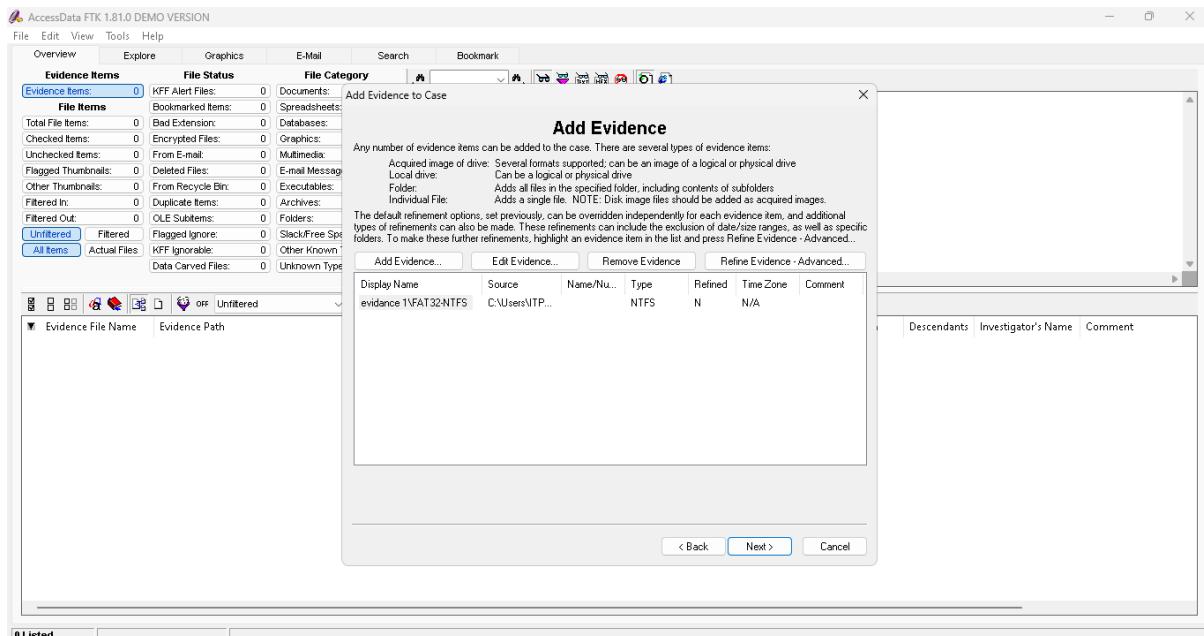
- Within Add Evidence Select evidence 1.dd and click on open



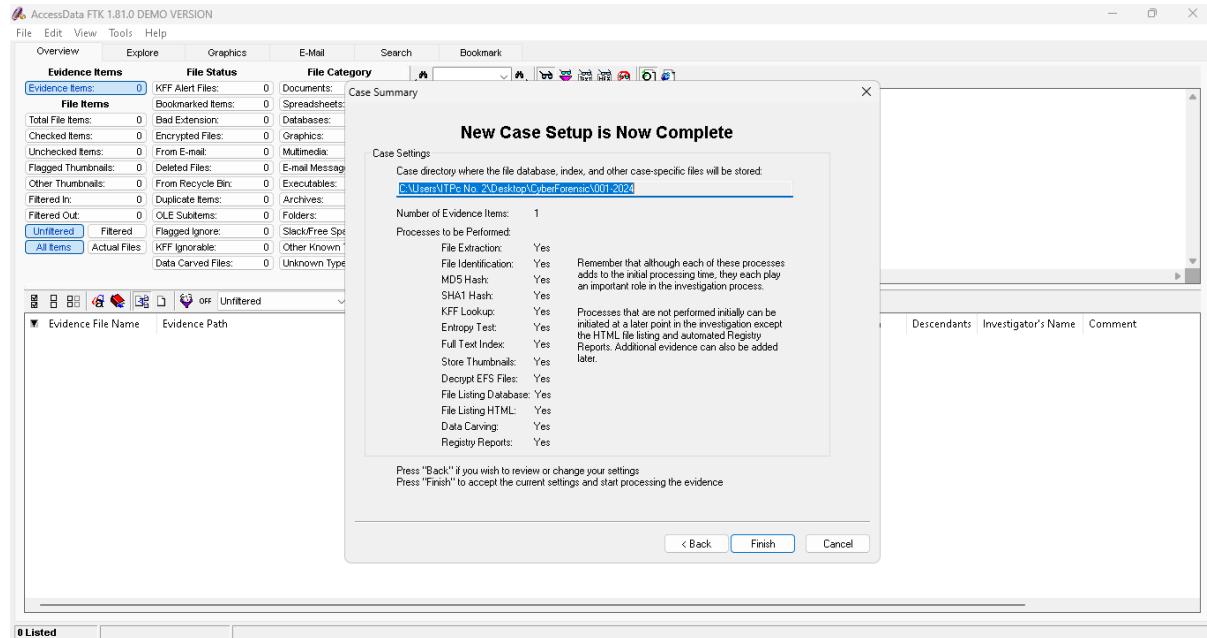
- Click on OK



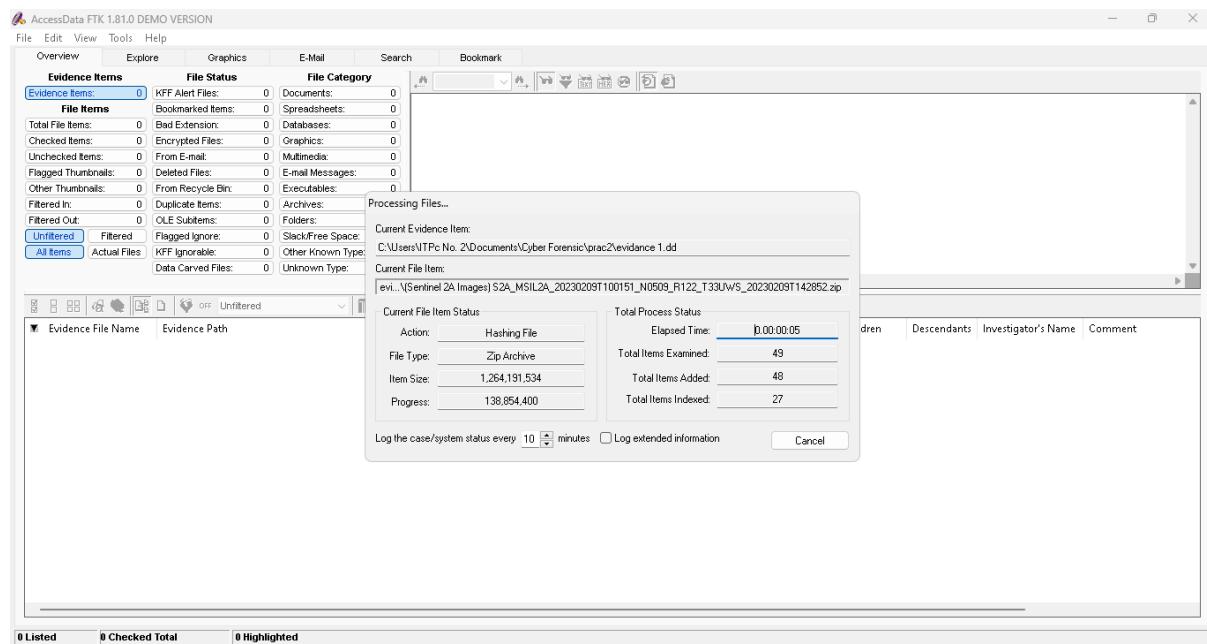
- Click on Next



- Click on Finish

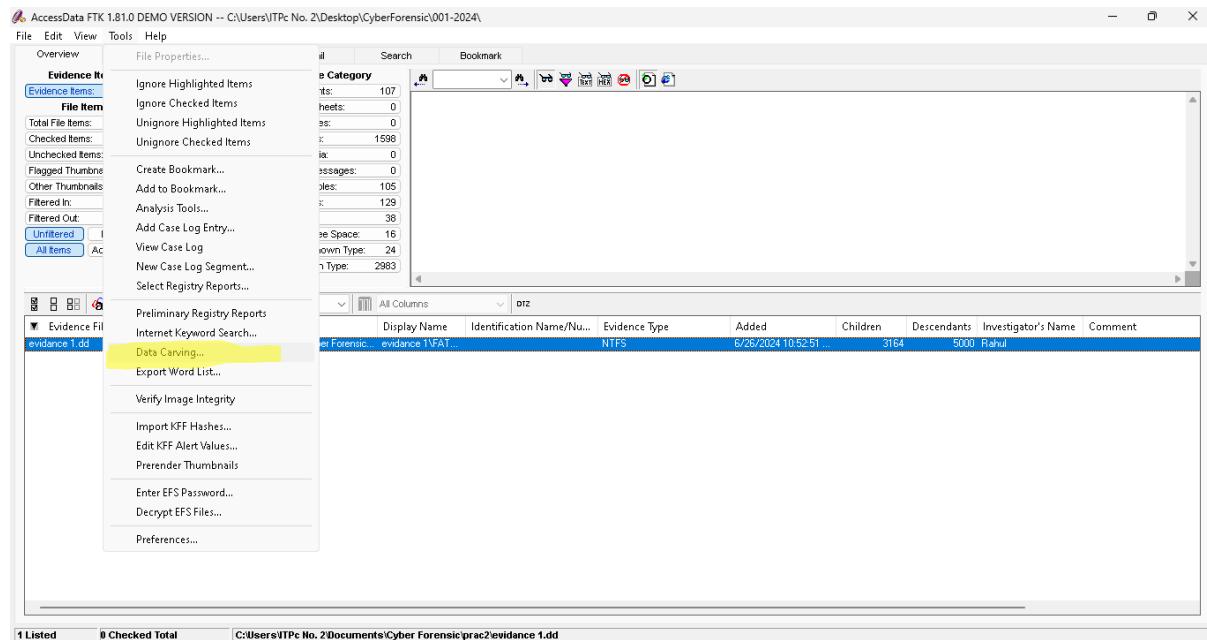


- It Start the Processing Files

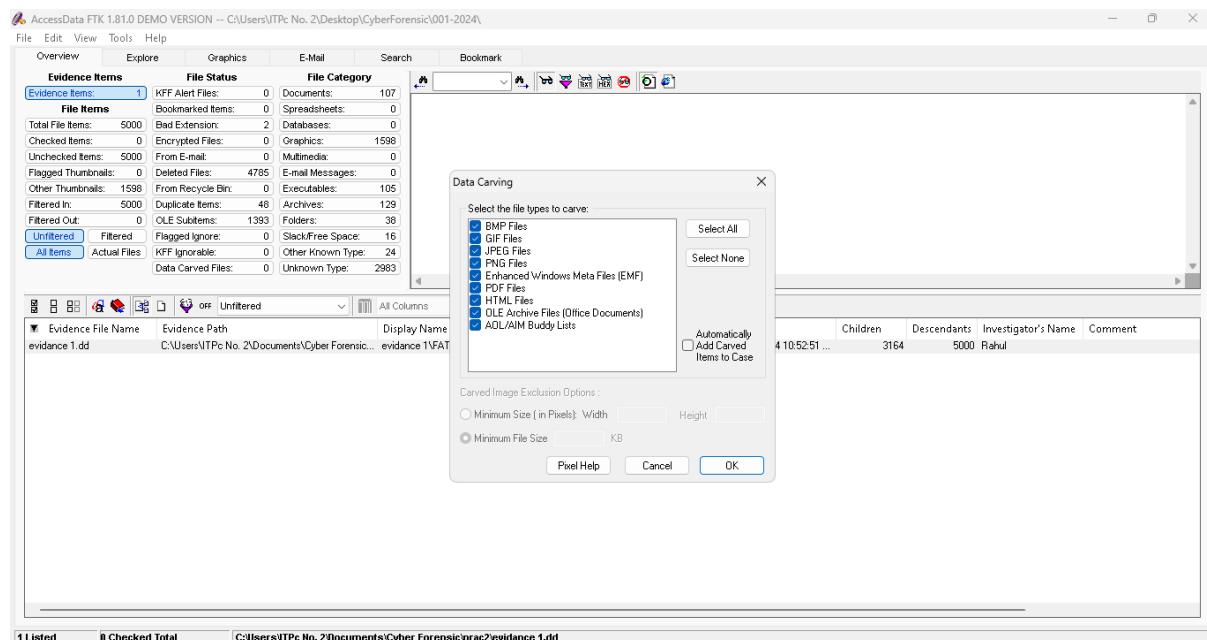


Step 8: Data Carving Files in an Existing Case

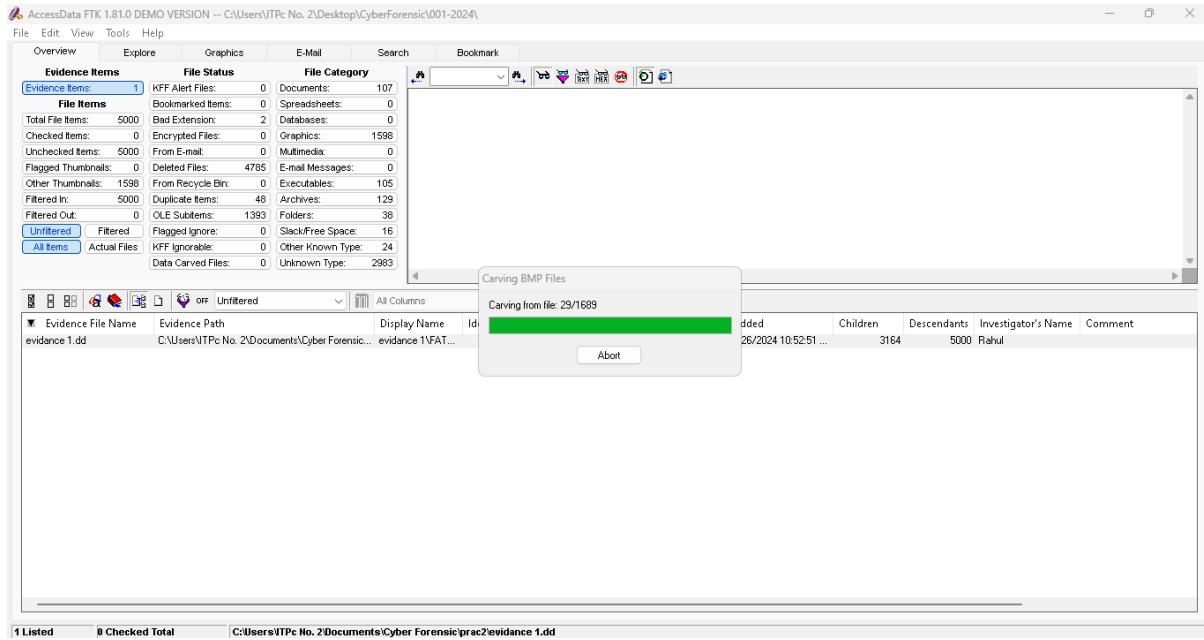
- Select Tools, and then Data Carving.



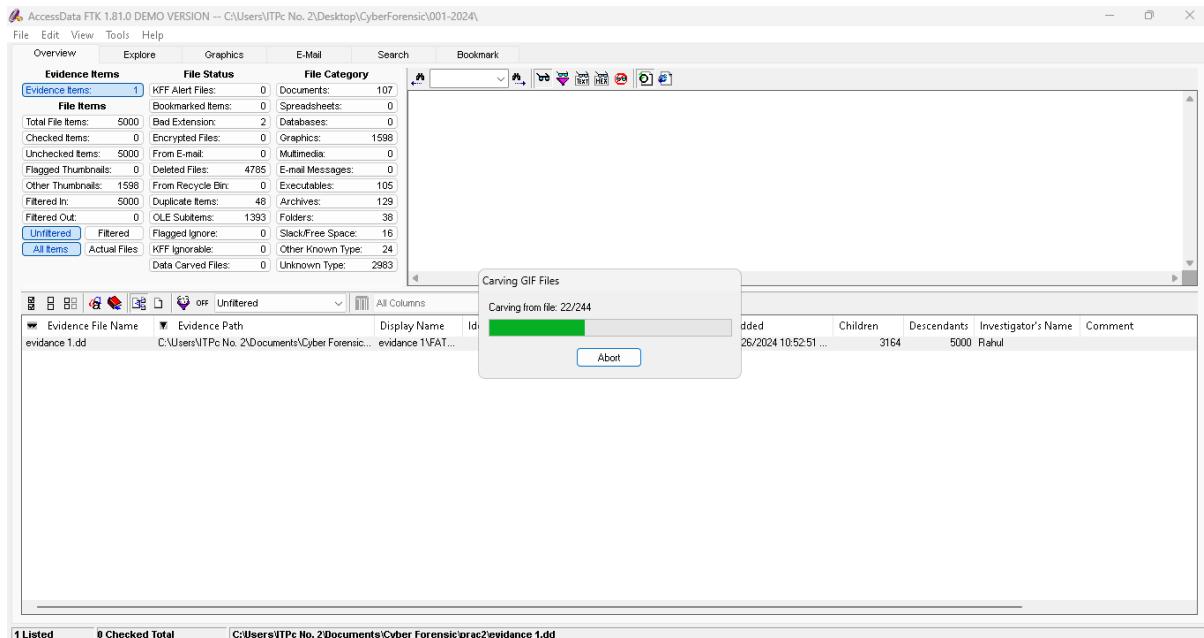
- Select BMP Files, GIF Files, and PNG Files and Click on OK



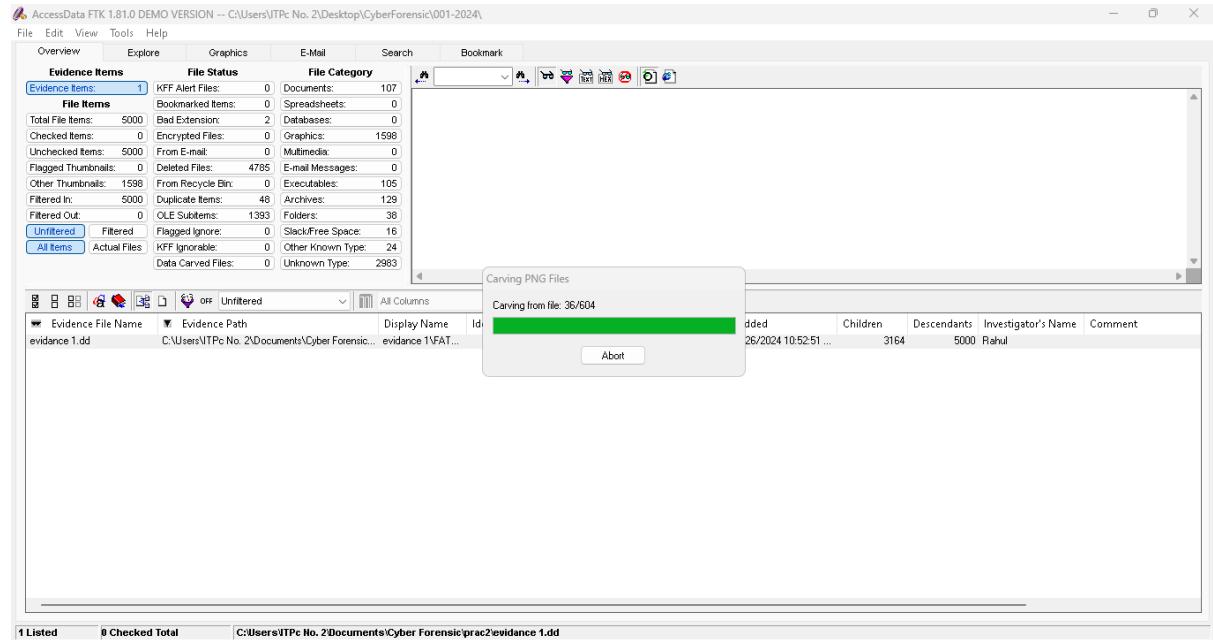
- It Will Start Carving BMP Files



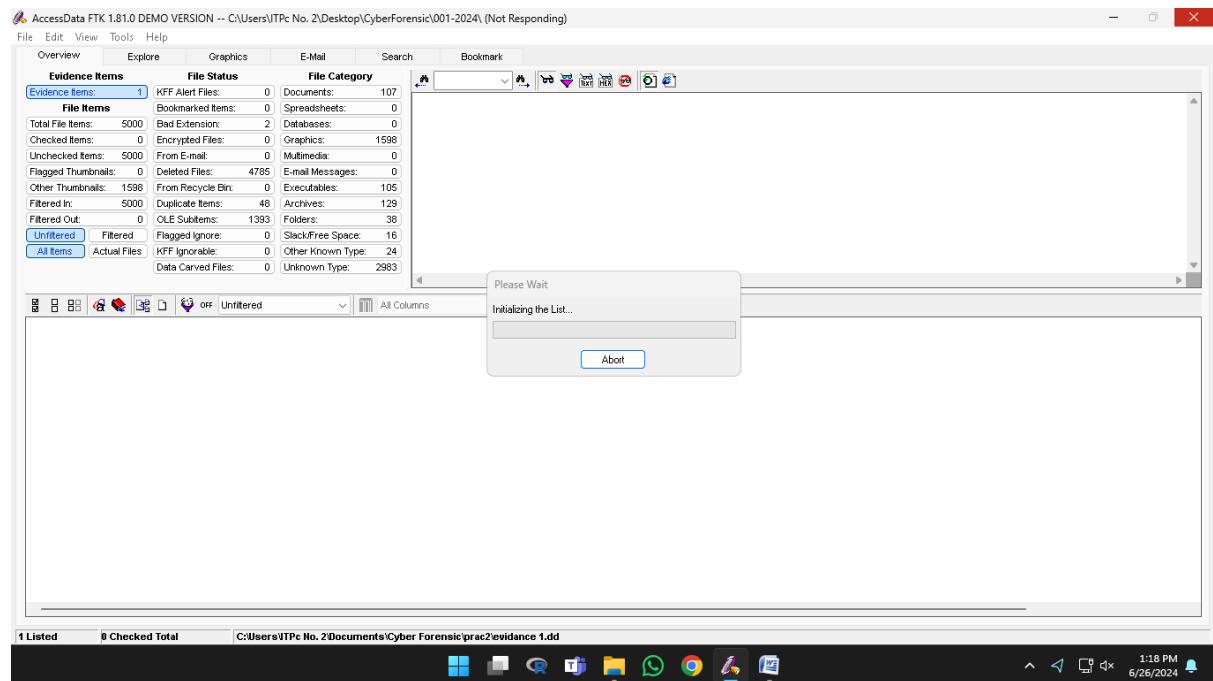
- After Carving BMP Files It Will Start Carving GIF Files



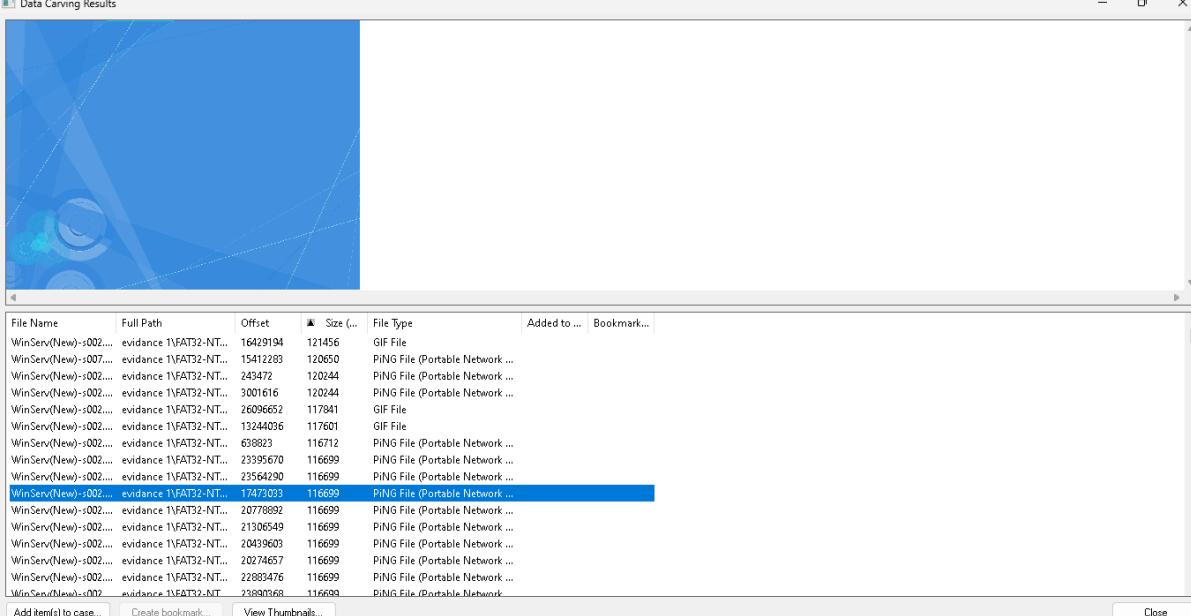
- After Carving BMP and GIF Files and then Next It Will Start Carving PNG Files



- After Carving BMP and GIF, PNG Files and then Next It Will Start Initializing the list



- After Initializing the list Here, We Can See the **Data Carving Results**

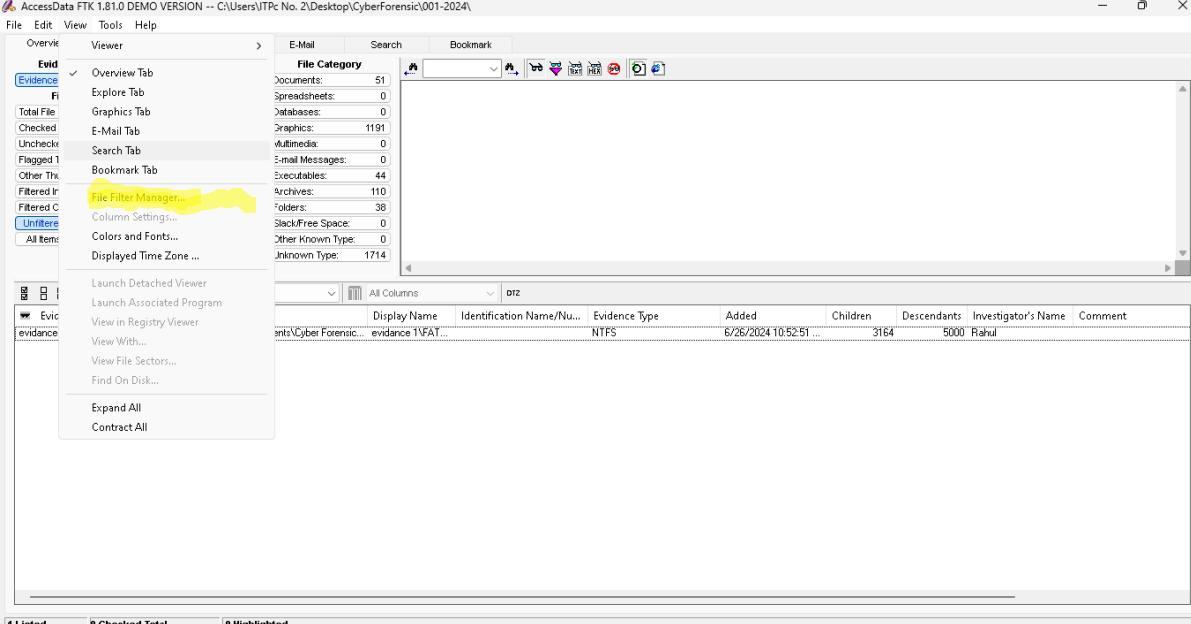


File Name	Full Path	Offset	Size (..)	File Type	Added to ...	Bookmark...
WinServ(New)->002....	evidence 1\FAT32-NT...	16429194	121456	GIF File		
WinServ(New)->007....	evidence 1\FAT32-NT...	15412283	120650	PING File (Portable Network ...		
WinServ(New)->002....	evidence 1\FAT32-NT...	243472	120244	PING File (Portable Network ...		
WinServ(New)->002....	evidence 1\FAT32-NT...	3001616	120244	PING File (Portable Network ...		
WinServ(New)->002....	evidence 1\FAT32-NT...	26096652	117841	GIF File		
WinServ(New)->002....	evidence 1\FAT32-NT...	13244036	117601	GIF File		
WinServ(New)->002....	evidence 1\FAT32-NT...	630823	116712	PING File (Portable Network ...		
WinServ(New)->002....	evidence 1\FAT32-NT...	23935670	116699	PING File (Portable Network ...		
WinServ(New)->002....	evidence 1\FAT32-NT...	23564290	116699	PING File (Portable Network ...		
WinServ(New)->002....	evidence 1\FAT32-NT...	17473031	116699	PING File (Portable Network ...		
WinServ(New)->002....	evidence 1\FAT32-NT...	20778892	116699	PING File (Portable Network ...		
WinServ(New)->002....	evidence 1\FAT32-NT...	21306549	116699	PING File (Portable Network ...		
WinServ(New)->002....	evidence 1\FAT32-NT...	20439603	116699	PING File (Portable Network ...		
WinServ(New)->002....	evidence 1\FAT32-NT...	20274657	116699	PING File (Portable Network ...		
WinServ(New)->002....	evidence 1\FAT32-NT...	22880476	116699	PING File (Portable Network ...		
WinServ(New)->002....	evidence 1\FAT32-NT...	23890368	116699	PING File (Portable Network ...		

Add item(s) to case... Create bookmark... View Thumbnails... Close

Step 9: Modifying or Creating a Filter

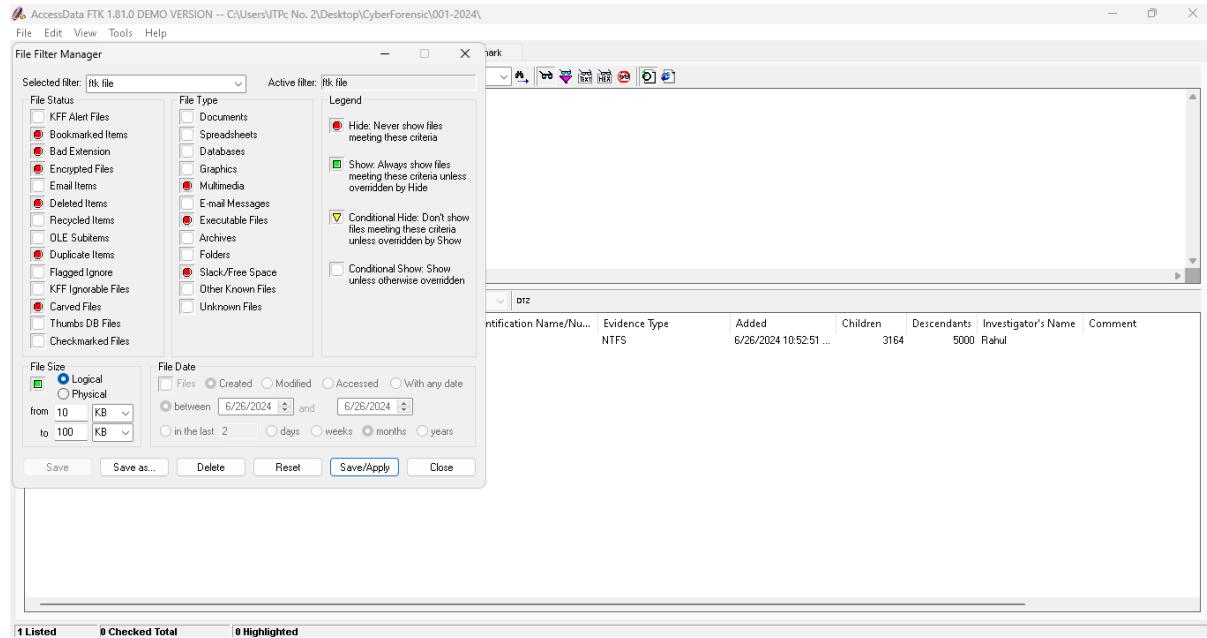
- Select View, and then File Filter Manager



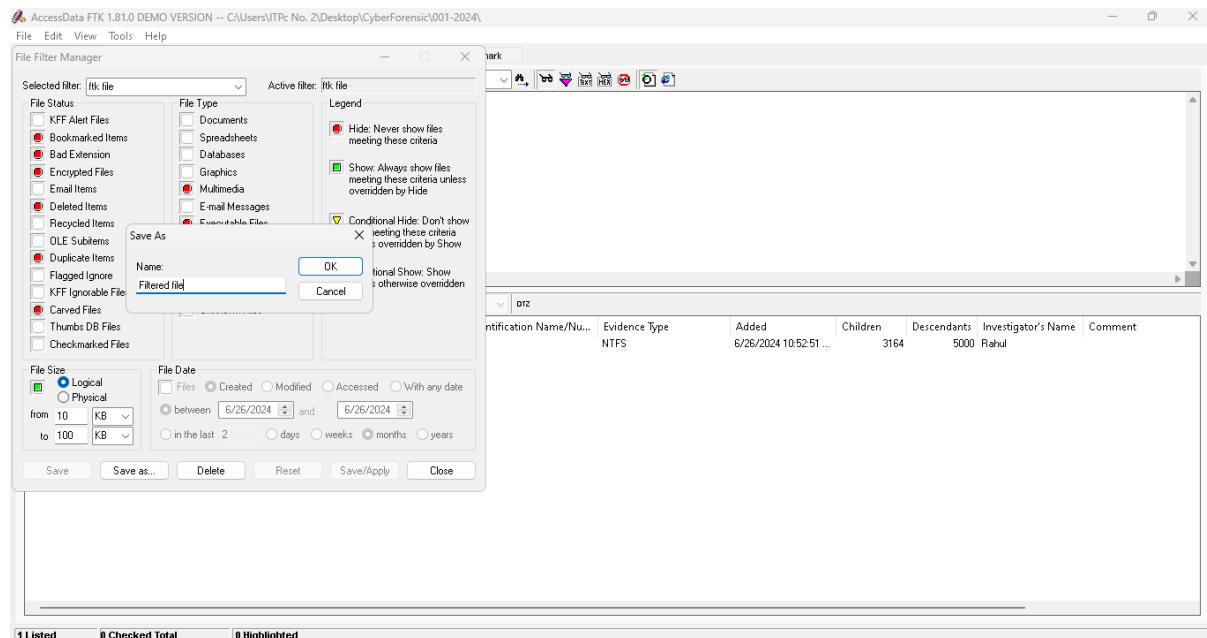
Display Name	Identification Name/Nu..	Evidence Type	Added	Children	Descendants	Investigator's Name	Comment
evidence 1\FAT...	NTFS	6/26/2024 10:52:51...	3164	5000	Rahul		

1 Listed 0 Checked Total 0 Highlighted

- Select the filter that you want to modify

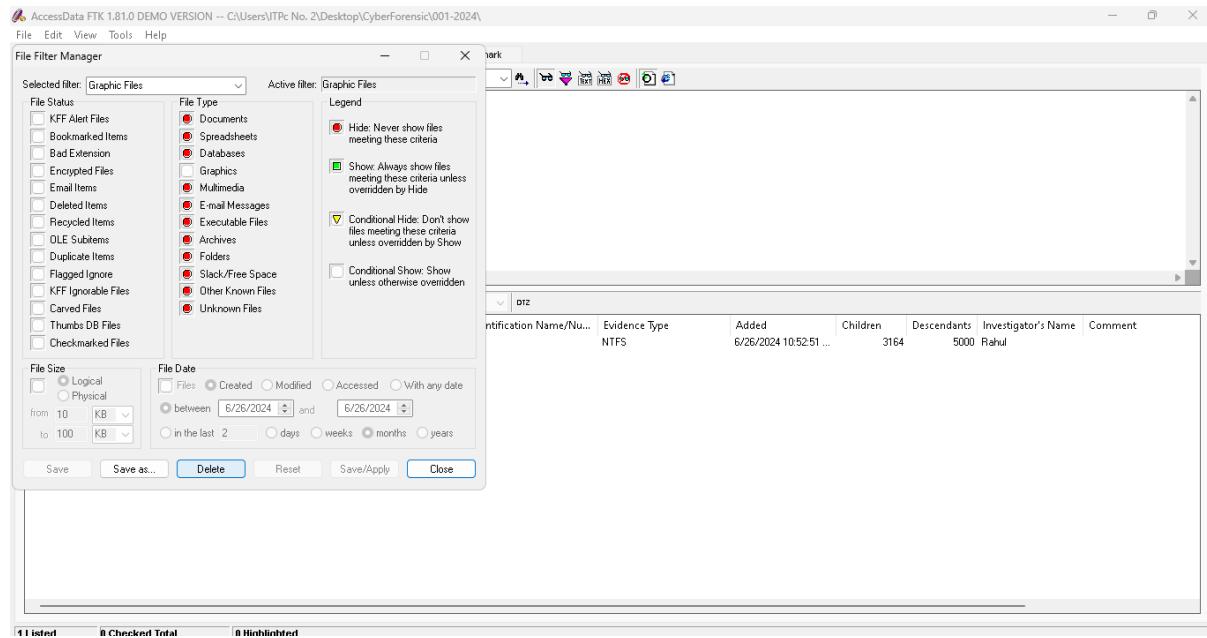


- If you are modifying an existing filter, click **Save/Apply**. Or If you are creating a new filter, click **Save As**, enter the name, and click **OK**.



Step 10: Deleting a Filter

- You can delete a filter if you no longer need it. To delete a filter:
- **Select View, and then File Filter Manager.**
- **Click Delete**

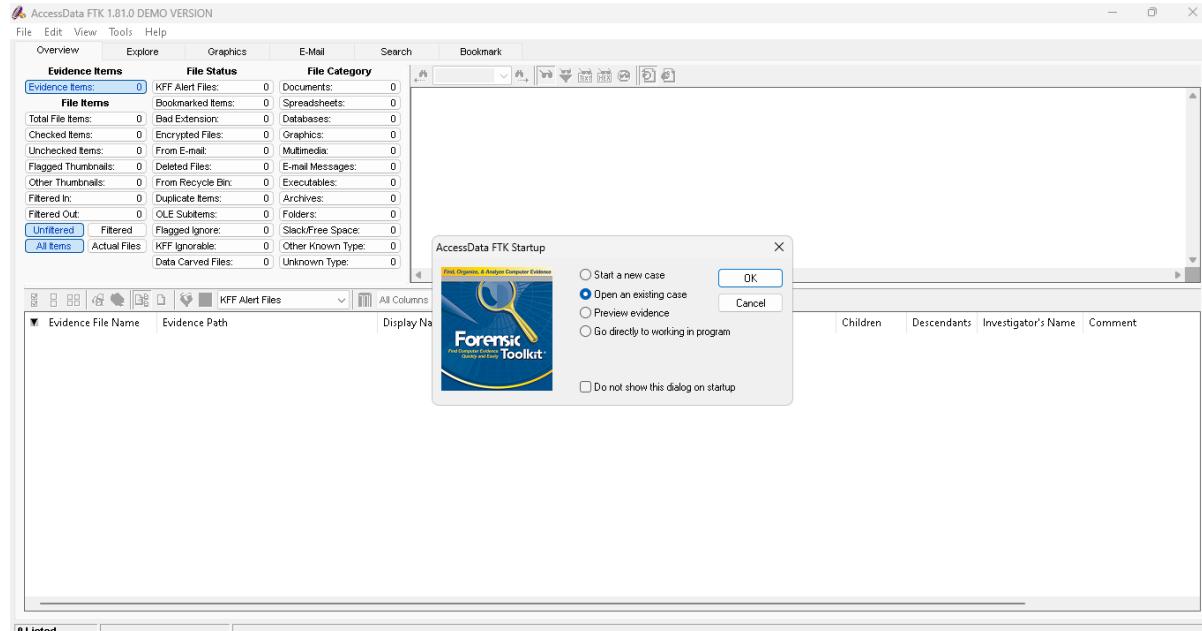


- Deleted Files

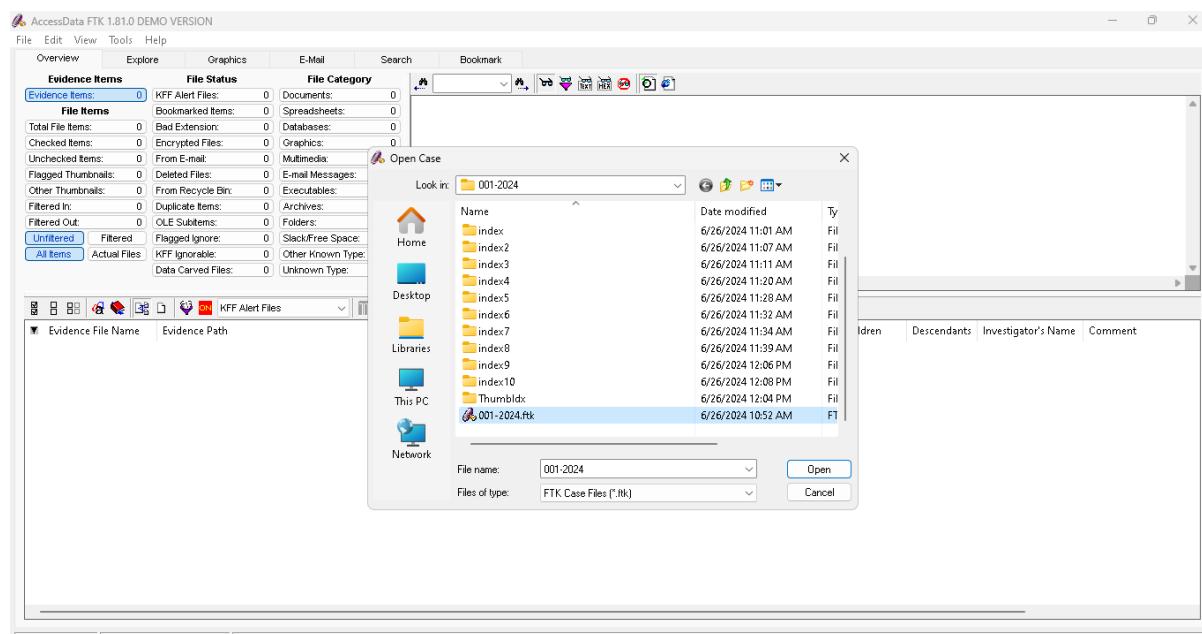
AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\UTPc No. 2\Desktop\CyberForensic\001-2024															
Evidence Items		File Status		File Category											
Evidence Items:	1	KFF Alert Files:	0	Documents:	0 <th>Bookmarked Items:</th> <td>0<th>Spreadsheets:</th><td>0</td><th>Databases:</th><td>0<th>Graphics:</th><td>1191</td><th>Multimedia:</th><td>0</td></td></td>	Bookmarked Items:	0 <th>Spreadsheets:</th> <td>0</td> <th>Databases:</th> <td>0<th>Graphics:</th><td>1191</td><th>Multimedia:</th><td>0</td></td>	Spreadsheets:	0	Databases:	0 <th>Graphics:</th> <td>1191</td> <th>Multimedia:</th> <td>0</td>	Graphics:	1191	Multimedia:	0
Total File Items:	1191	Bad Extension:	0	Executables:	0	OLE Subtypes:	0	Archives:	0	ZIP:	0	OLE Container:	0	OLE Objects:	0
Checked Items:	1	Encrypted Files:	0	Text Files:	0	From E-mail:	0	Multimedia:	0	Word Processing:	0	Image Files:	0	PDF:	0
Unchecked Items:	1190	From Recycle Bin:	0	HTML:	0	From Network:	0	Scripting:	0	XML:	0	Database:	0	OLE Container:	0
Flagged Thumbnails:	0	Deleted Files:	1191	E-mail Messages:	0	File Carved:	0	OLE Subtypes:	0	OLE Objects:	0	OLE Container:	0	OLE Objects:	0
Other Thumbnails:	1191	From Recycle Bin:	0	Executable:	0	File Carved:	0	Archives:	0	OLE Container:	0	OLE Container:	0	OLE Container:	0
Filtered In:	1191	Duplicate Items:	2	Archives:	0	File Carved:	0	ZIP:	0	OLE Container:	0	OLE Container:	0	OLE Container:	0
Filtered Out:	1957	OLE Subtypes:	0	Archives:	0	File Carved:	0	ZIP:	0	OLE Container:	0	OLE Container:	0	OLE Container:	0
Unfiltered:	Filtered	Flagged Ignore:	0	Slack/Free Space:	0	File Carved:	0	OLE Objects:	0	OLE Container:	0	OLE Container:	0	OLE Container:	0
All Items:	Actual File	KFF Ignorable:	0	Other Known Type:	0	File Carved:	0	Unknown Type:	0	OLE Container:	0	OLE Container:	0	OLE Container:	0
File Filter Manager															
File Name															
admin_band.gif	evidence 1\FA\32\NTFS\w2010\Setup\admin...	gl	GIF File	Graphic	1/9/2024 10:34:52 AM	3/12/2010 7:12:18 AM	1/9/2024 10:34:52 AM	986	4,096						
admin_band.bmp	evidence 1\FA\32\NTFS\w2010\Setup\admin...	bmp	Bitmap File	Graphic	1/9/2024 10:34:52 AM	3/12/2010 7:12:20 AM	1/9/2024 10:34:52 AM	63,480	65,536						
banner.bmp	evidence 1\FA\32\NTFS\w2010\Setup\banner...	bmp	Bitmap File	Graphic	1/9/2024 10:34:52 AM	3/12/2010 7:12:20 AM	1/9/2024 10:34:52 AM	63,480	65,536						
banner_blank.bmp	evidence 1\FA\32\NTFS\w2010\Setup\banner...	bmp	Bitmap File	Graphic	1/9/2024 10:34:52 AM	3/12/2010 7:12:08 AM	1/9/2024 10:34:52 AM	1,398	4,096						
big_info.png	evidence 1\FA\32\NTFS\w2010\Setup\big_info...	png	PNG File (Po...	Graphic	1/9/2024 10:34:52 AM	12/5/2009 2:49:04 PM	1/9/2024 10:34:52 AM	1,563	4,096						
blueRule.gif	evidence 1\FA\32\NTFS\w2010\Setup\blueRu...	gl	GIF File	Graphic	1/9/2024 10:34:52 AM	3/12/2010 7:12:18 AM	1/9/2024 10:34:52 AM	815	4,096						
bullet.png	evidence 1\FA\32\NTFS\w2010\Setup\bullet.p...	png	PNG File (Po...	Graphic	1/9/2024 10:34:52 AM	10/17/2008 8:38:34	1/9/2024 10:34:52 AM	1,259	4,096						
divider0.jpg	evidence 1\FA\32\NTFS\w2010\Setup\divider...	jpg	JPEG/JIFF File	Graphic	1/9/2024 10:34:52 AM	3/12/2010 7:12:18 AM	1/9/2024 10:34:52 AM	367	36						
greenRule.gif	evidence 1\FA\32\NTFS\w2010\Setup\green...	gl	GIF File	Graphic	1/9/2024 10:34:52 AM	3/12/2010 7:12:18 AM	1/9/2024 10:34:52 AM	44	44						
info-icon.png	evidence 1\FA\32\NTFS\w2010\Setup\info-ico...	png	PNG File (Po...	Graphic	1/9/2024 10:34:52 AM	12/5/2009 2:49:04 PM	1/9/2024 10:34:52 AM	3,424	4,096						
install_button.png	evidence 1\FA\32\NTFS\w2010\Setup\install...	png	PNG File (Po...	Graphic	1/9/2024 10:34:52 AM	12/5/2009 2:49:04 PM	1/9/2024 10:34:52 AM	4,076	4,096						
large_info.png	evidence 1\FA\32\NTFS\w2010\Setup\large_i...	png	PNG File (Po...	Graphic	1/9/2024 10:34:52 AM	3/12/2010 7:12:18 AM	1/9/2024 10:34:52 AM	3,126	4,096						
mant_band.bmp	evidence 1\FA\32\NTFS\w2010\Setup\mant...	bmp	Bitmap File	Graphic	1/9/2024 10:34:52 AM	3/12/2010 7:12:20 AM	1/9/2024 10:34:52 AM	63,480	65,536						
redRule.gif	evidence 1\FA\32\NTFS\w2010\Setup\redRu...	gl	GIF File	Graphic	1/9/2024 10:34:53 AM	3/12/2010 7:12:18 AM	1/9/2024 10:34:53 AM	44	44						
Screenshot (120).png	evidence 1\FA\32\NTFS\w2010\Files\Screenshot...	png	PNG File (Po...	Graphic	12/23/2023 12:45:01...	10/21/2023 2:44:38...	12/23/2023 8:40:18...	160,871	163,840						
Screenshot (121).png	evidence 1\FA\32\NTFS\w2010\Files\Screenshot...	png	PNG File (Po...	Graphic	12/23/2023 12:45:01...	10/21/2023 2:45:05...	12/23/2023 8:40:18...	144,740	147,456						
Screenshot (122).png	evidence 1\FA\32\NTFS\w2010\Files\Screenshot...	png	PNG File (Po...	Graphic	12/23/2023 12:45:01...	10/21/2023 2:45:09...	12/23/2023 8:40:18...	123,352	131,072						
Screenshot (123).png	evidence 1\FA\32\NTFS\w2010\Files\Screenshot...	png	PNG File (Po...	Graphic	12/23/2023 12:45:01...	10/21/2023 2:45:17...	12/23/2023 8:40:18...	154,920	155,648						
Screenshot (124).png	evidence 1\FA\32\NTFS\w2010\Files\Screenshot...	png	PNG File (Po...	Graphic	12/23/2023 12:45:01...	10/21/2023 2:45:49...	12/23/2023 8:40:19...	145,757	147,456						

Step 12: Searching the Registry

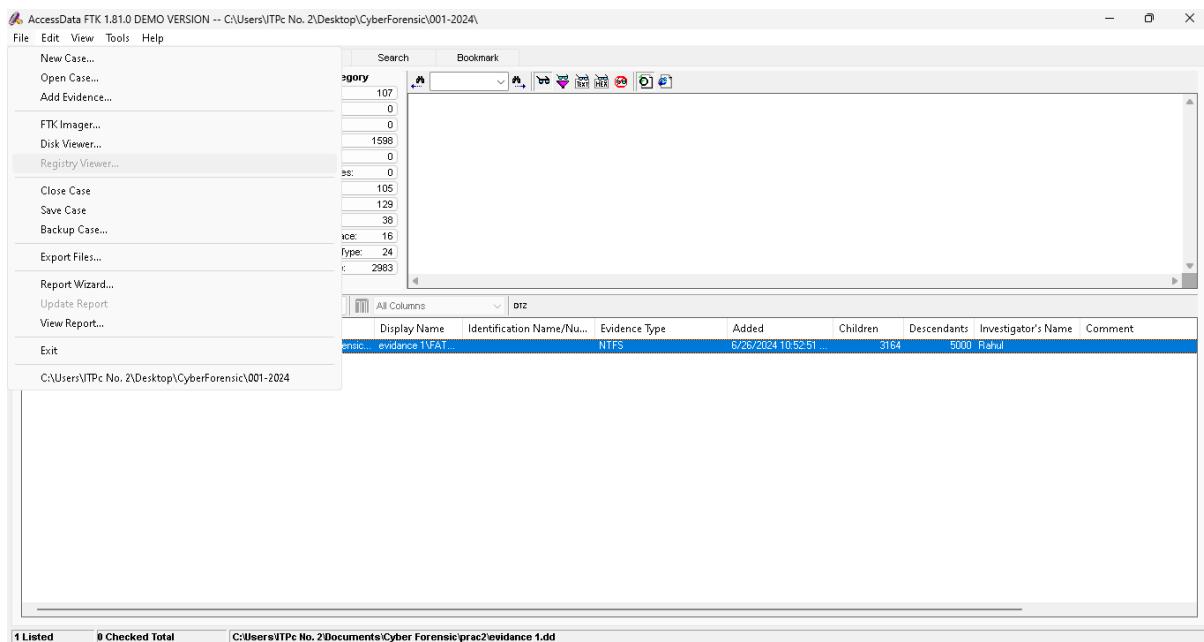
- **Launching Registry Viewer as a Separate Application:**
- To run Registry Viewer as a separate application, select Start, then Programs, then AccessData, and then Registry Viewer, and then Registry Viewer
- Launching Registry Viewer from FTK:
- To run Registry Viewer from FTK:
- In FTK, open an existing case by selecting File, and then Open Case.
- Or if you have chosen to always display the FTK Startup screen, select Open an Existing Case and click OK



- Select the case you want to open.

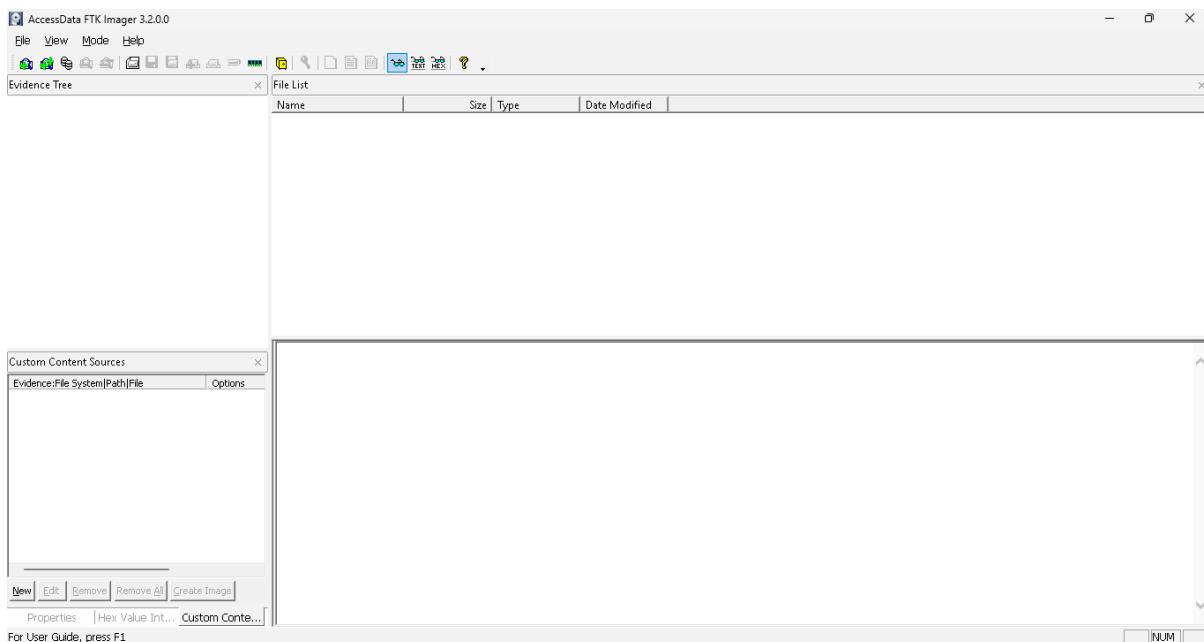


- Select File, and then Registry Viewer to open Registry Viewer.
- (Can't perform ahead of this step because Registry viewer is disabled in demo version)

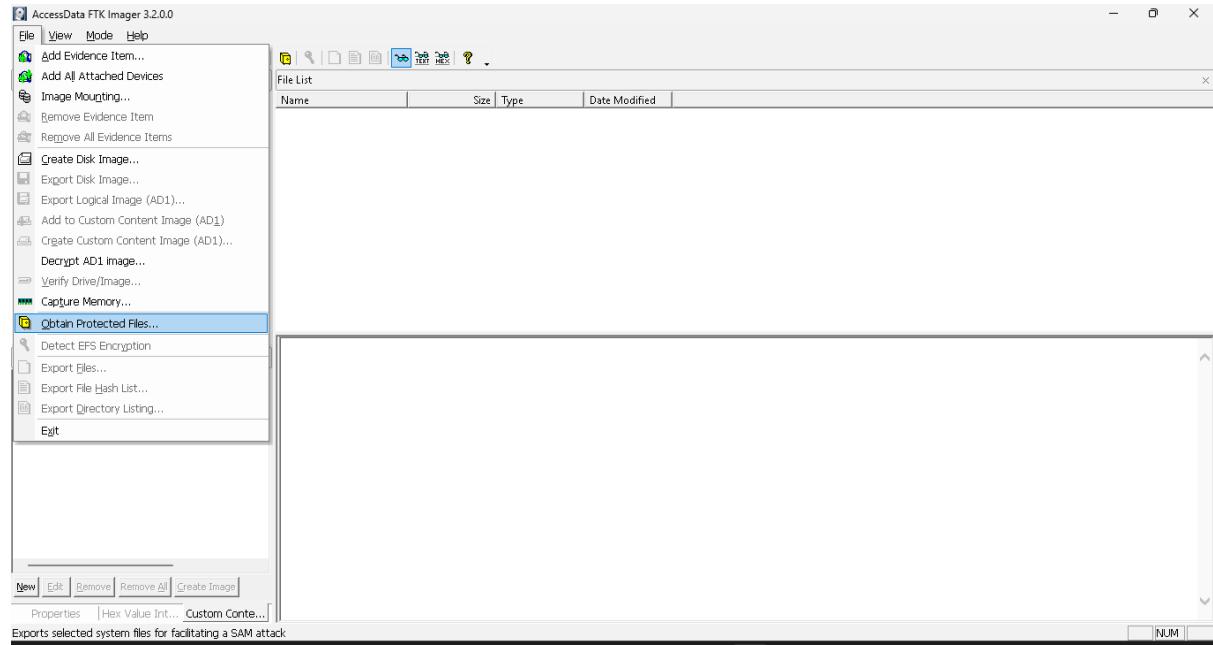


Step 13: Obtaining Protected Registry Files Using FTK Imager

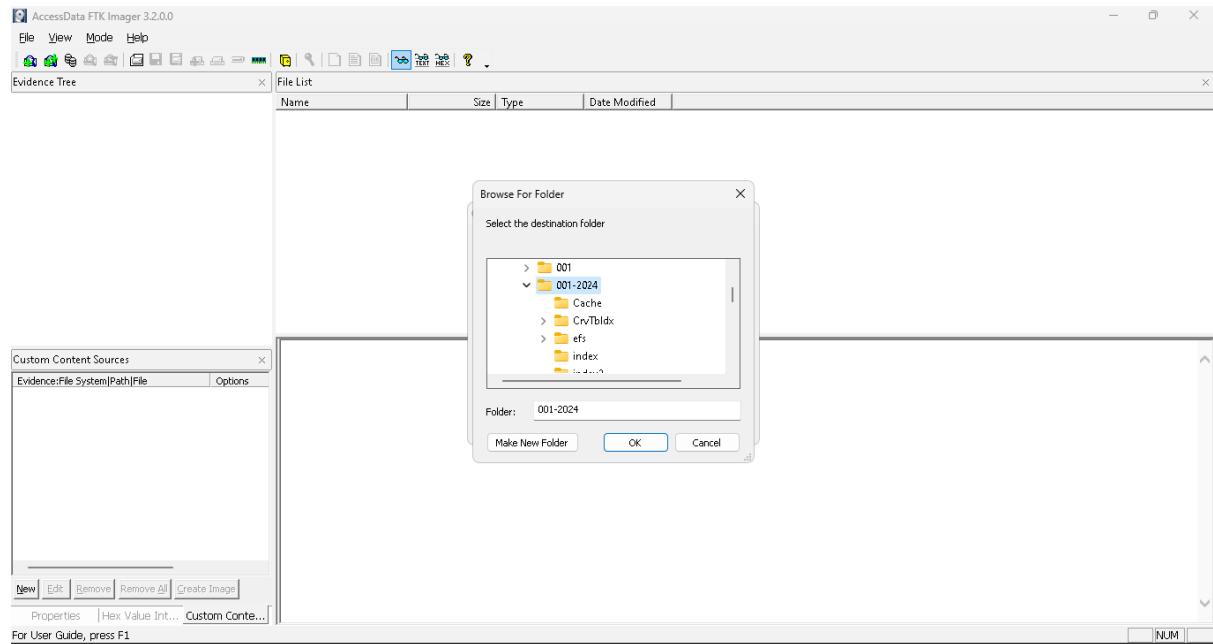
- To obtain the protected registry files using FTK Imager:
- Launch FTK Imager.



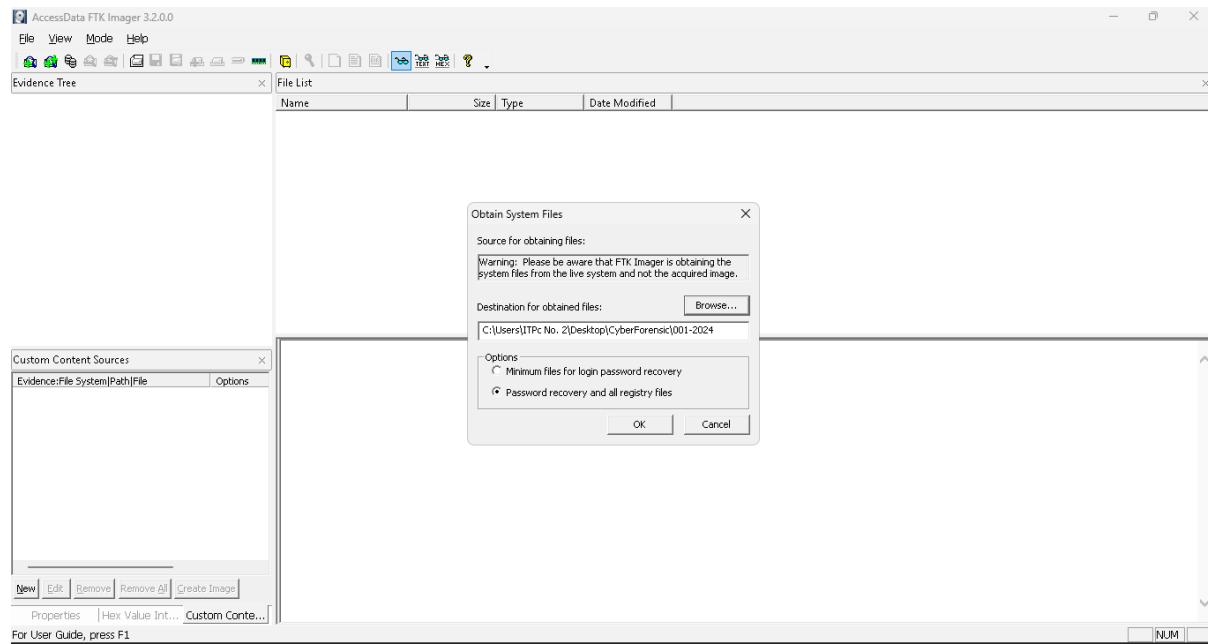
- Click File, and then Obtain Protected Files



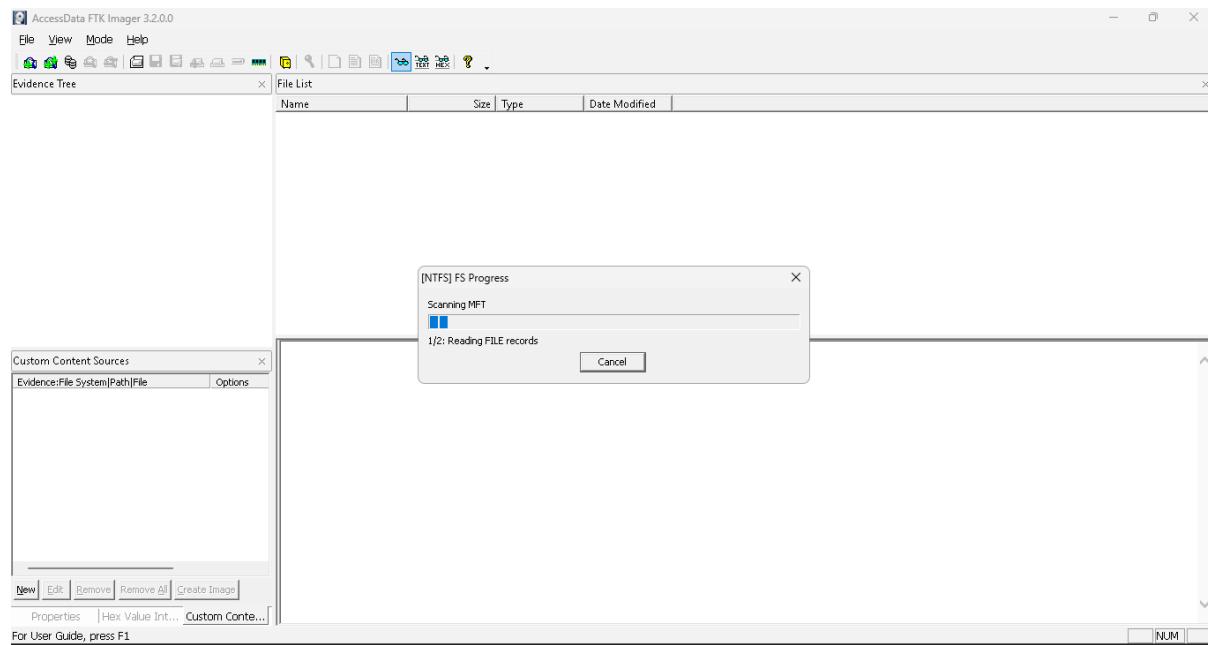
- Select the destination folder (Here it is 001-2024) and Click on OK



- Under System Files Options Select Password recovery and all registry files and Click on OK

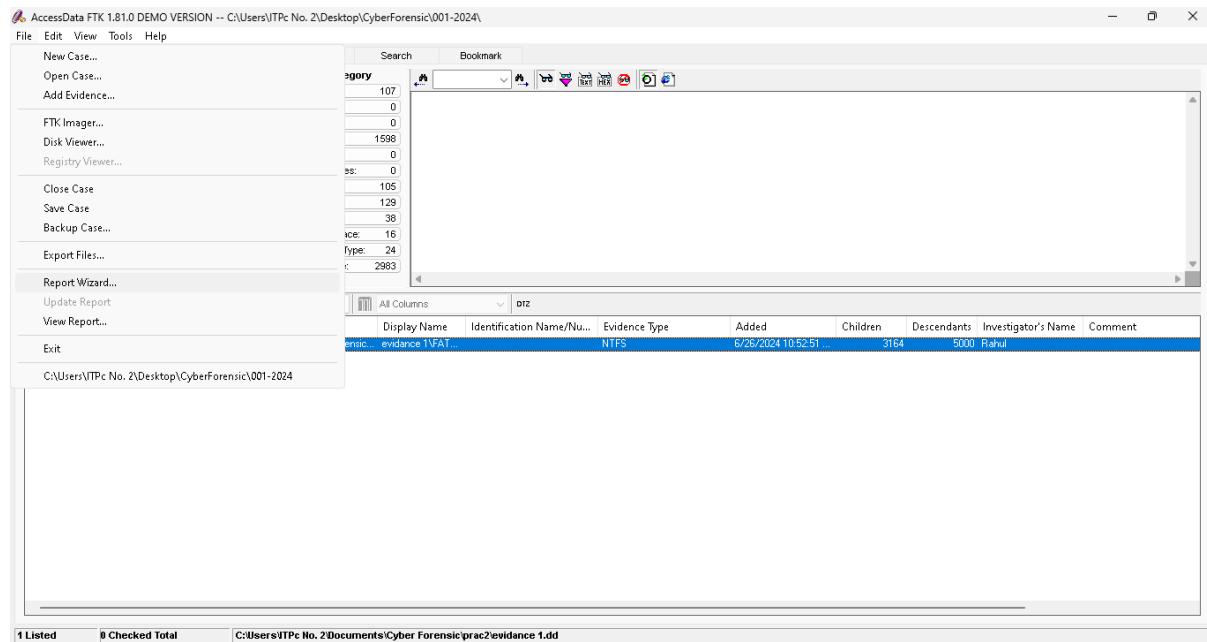


- Scanning MFT

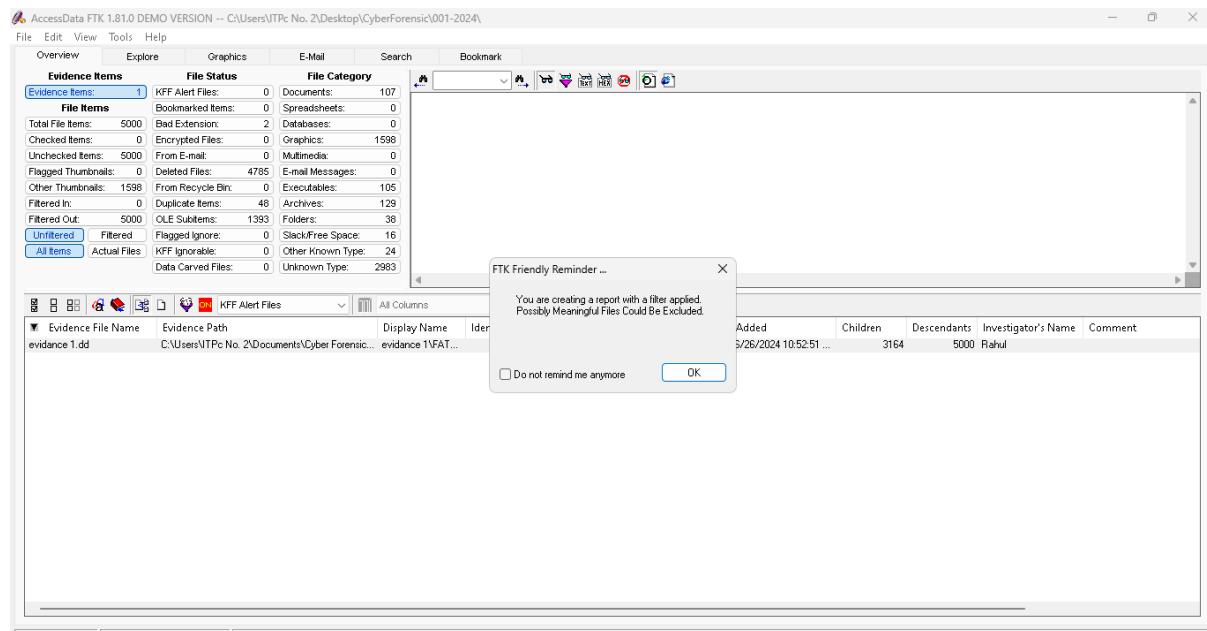


Step 14: Generating a Report

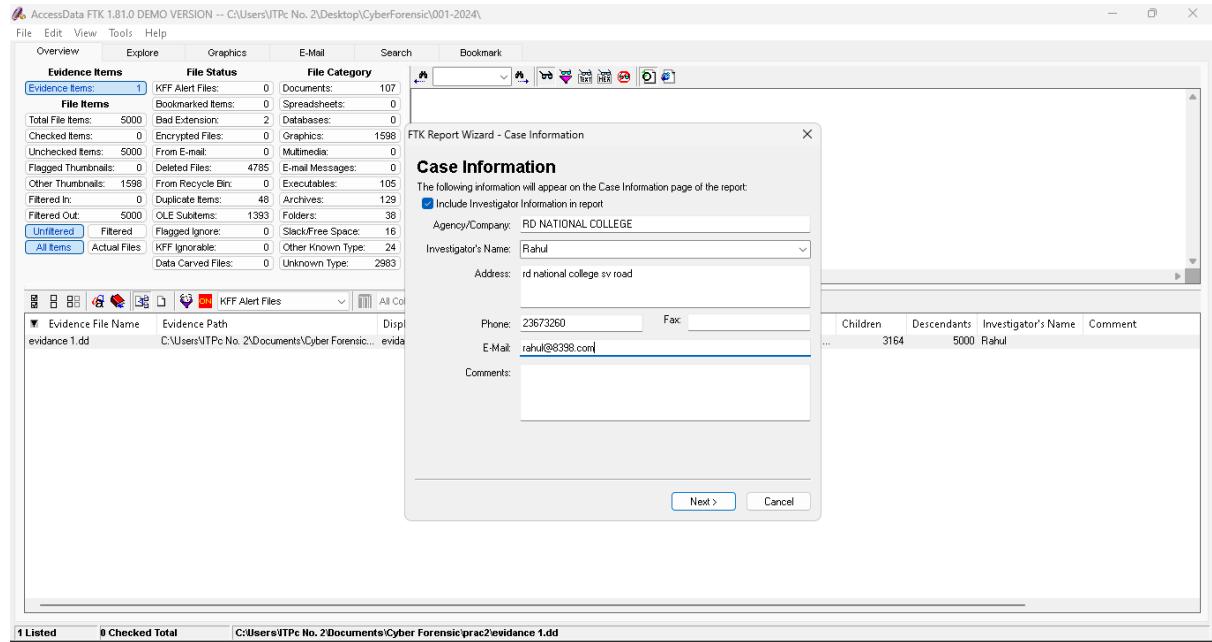
- From the menu, select **Report**, and then **Generate Report** or click the button on the toolbar



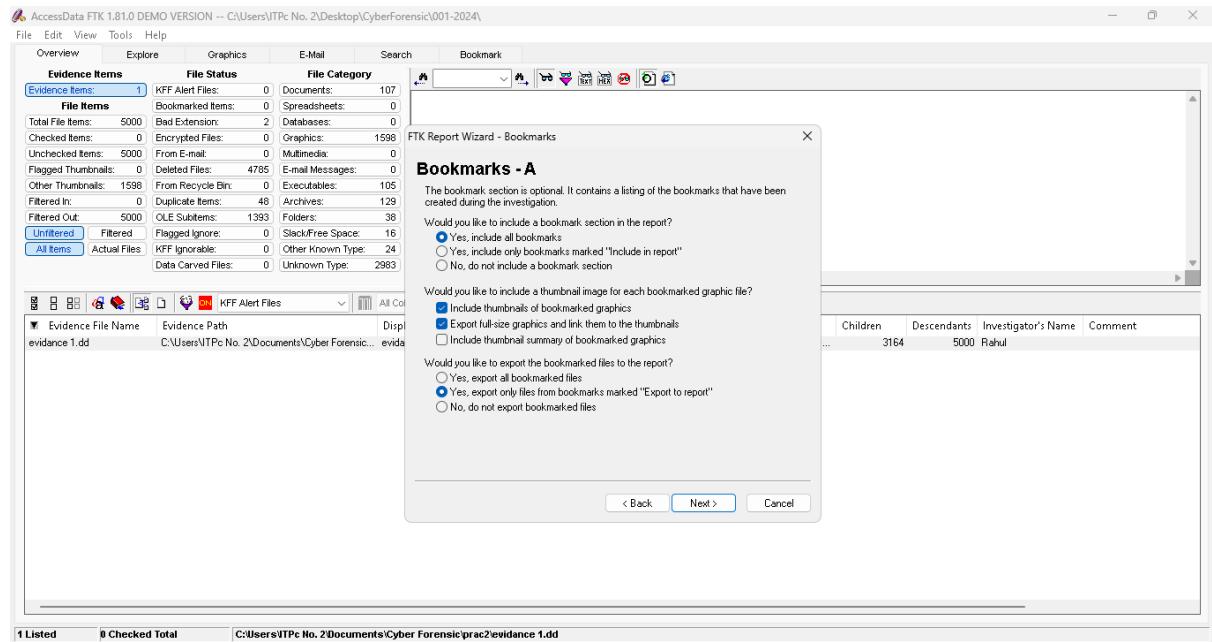
- Click on OK



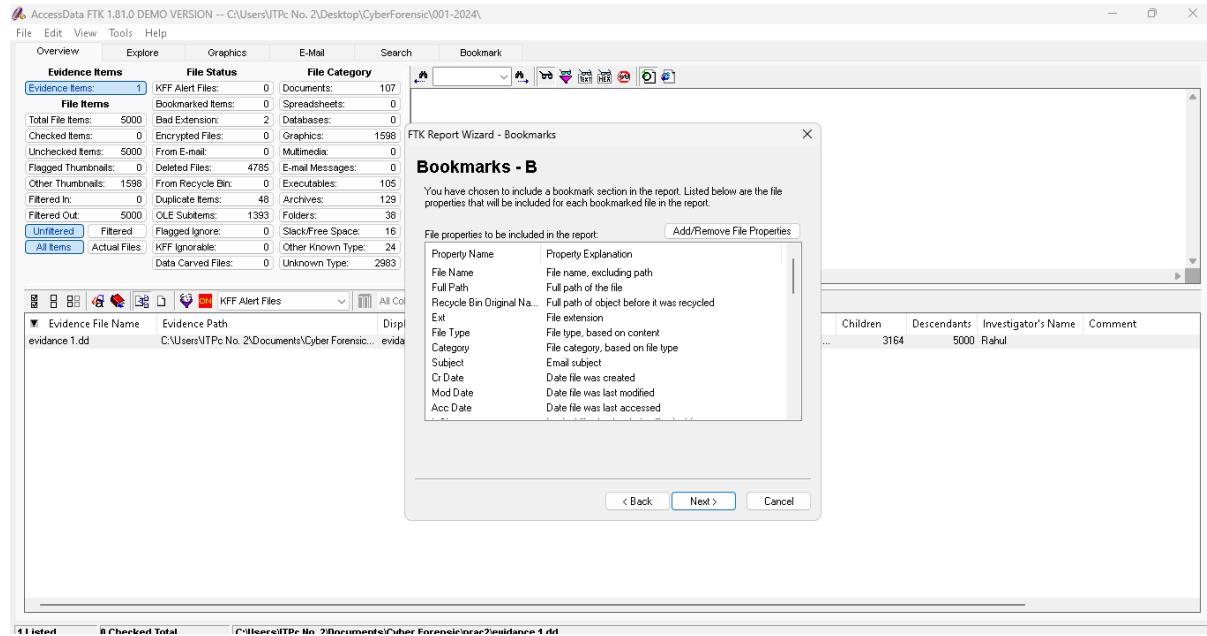
- Under Case Information Enter Following Information and Click on Next



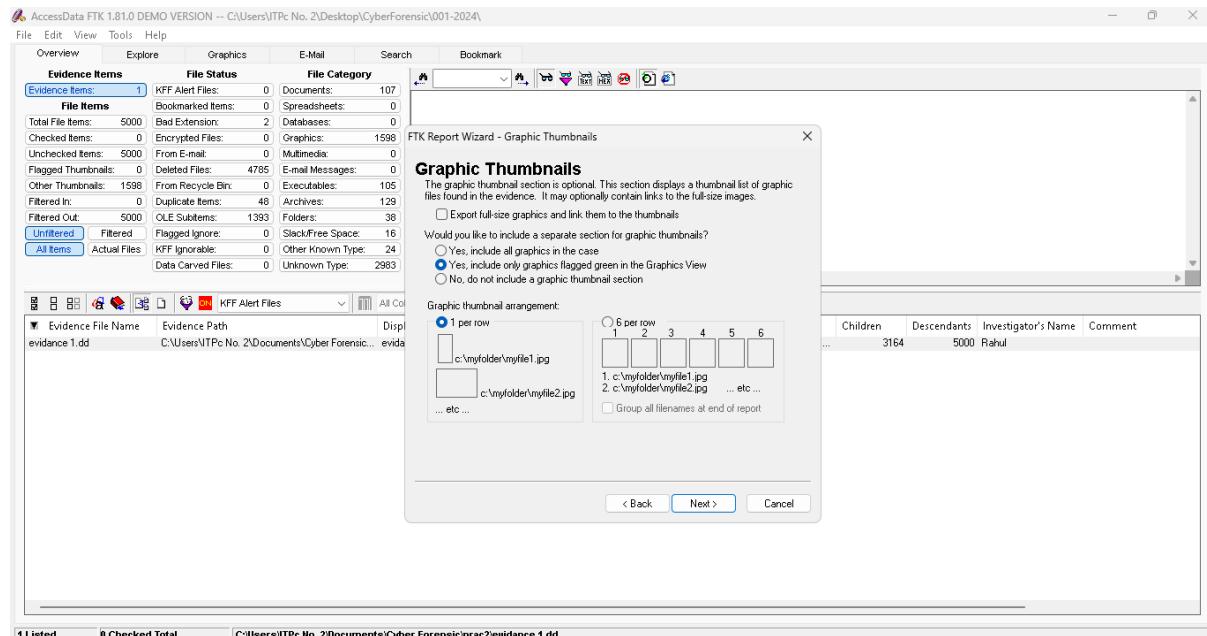
- Keep the Default Setting and Click on Next



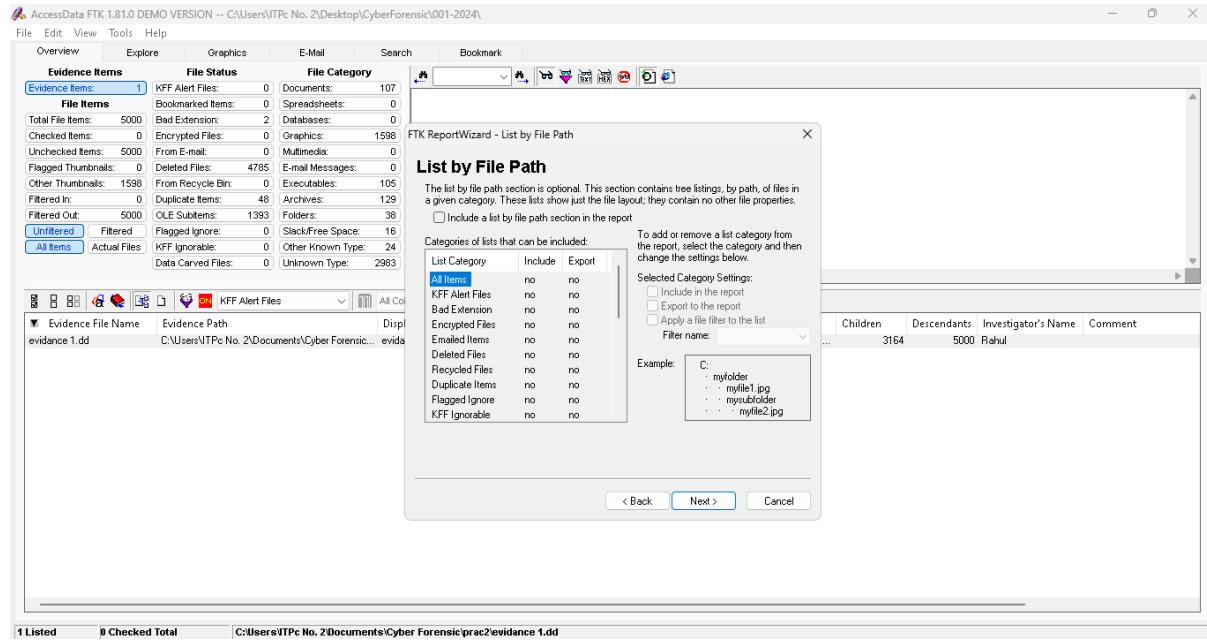
- Keep the Default Setting and Click on Next



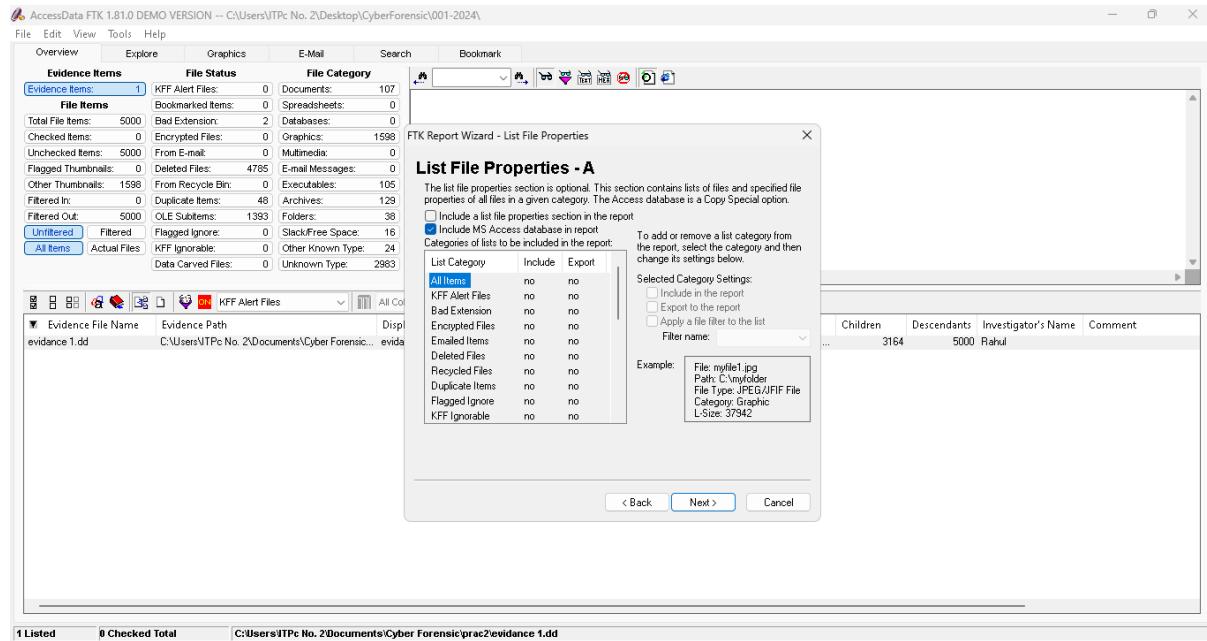
- Keep the Default Setting and Click on Next



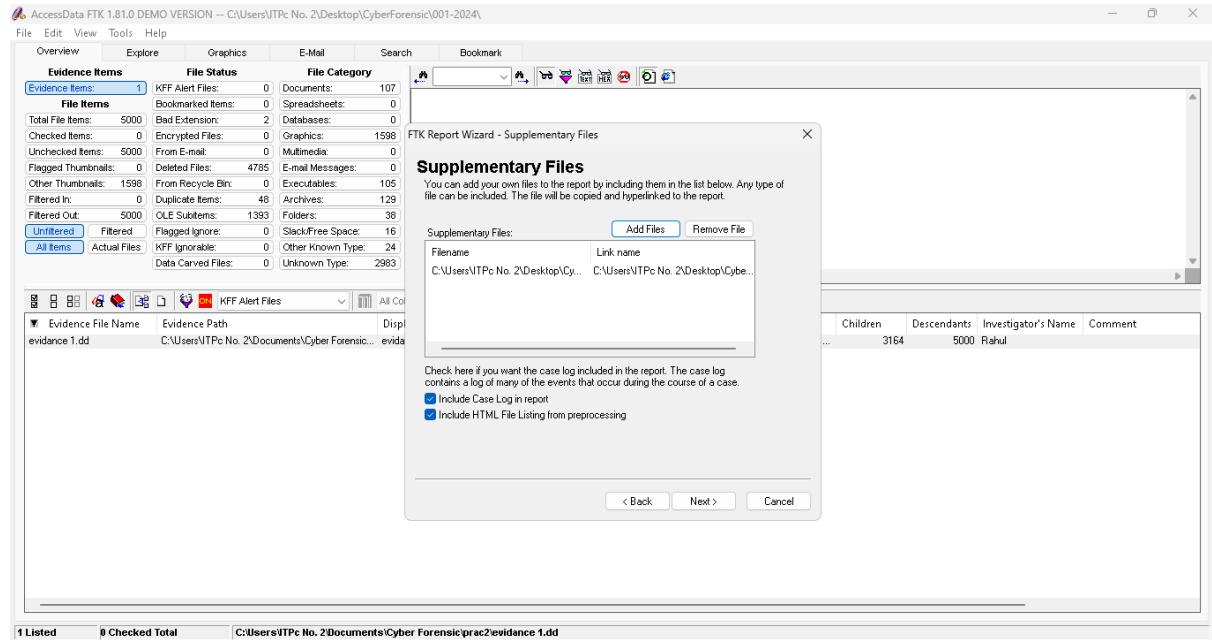
- Click on Next



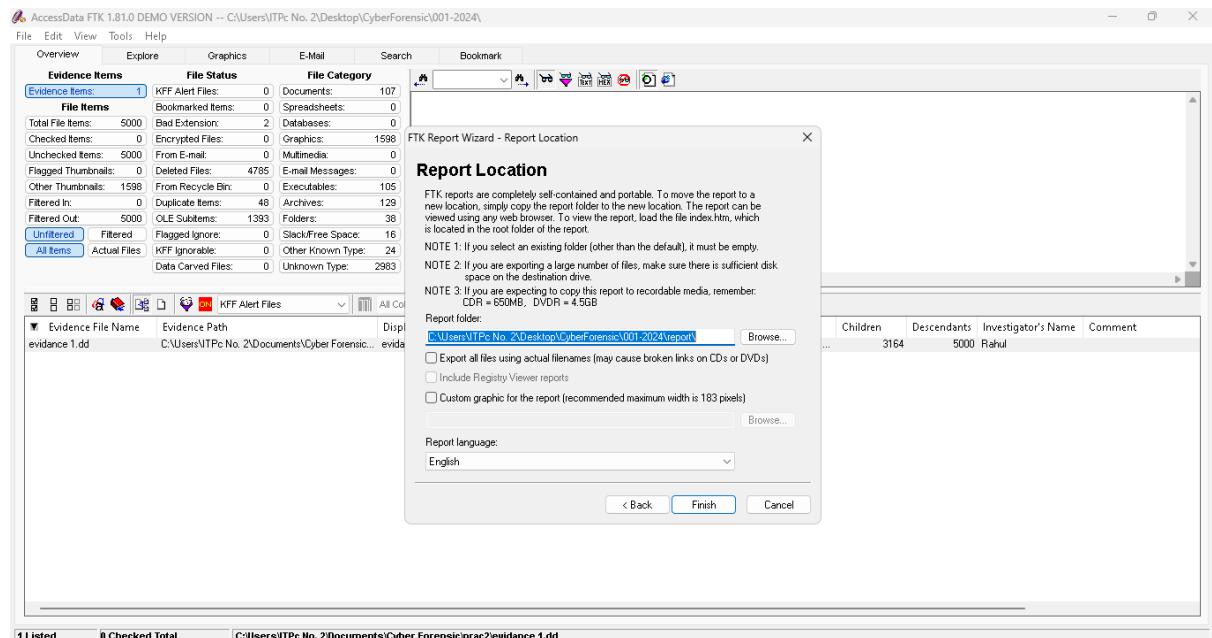
- Click on Next



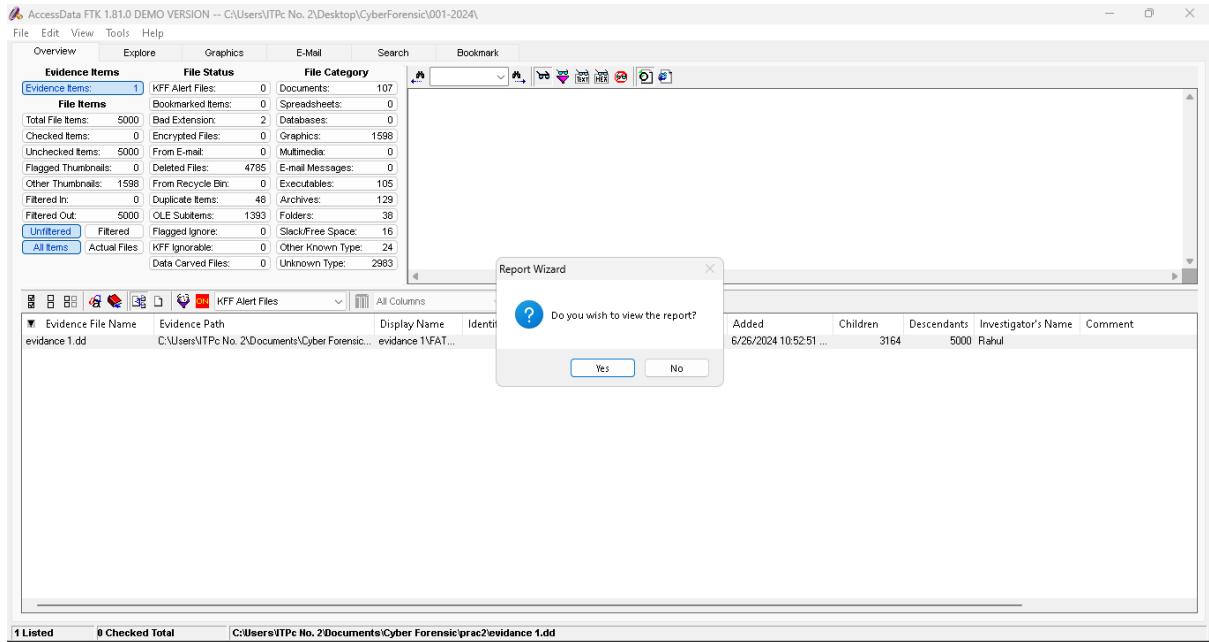
- Click on Add Files and Select the Supplementary Files and Click on Next



- Click on Finish



- Click on OK



- Generated Report

The screenshot shows the 'Case Information' page of the FTK Case Report. It displays the following details:

- Case Summary:**
 - Case Number: 001
 - Case Location: C:\Users\ITPc No. 2\Desktop\CyberForensic\001-2024
 - Case Description: CyberForensic Investigation
 - Report Created: Wednesday, June 26, 2024 2:10:35 PM
- Supplementary Files:**
 - 001-2024.ftk
 - Case Log
 - HTML File Listing
- List by File Path:** - None -
 - Forensic Examiner
 - Agency
 - Address
 - Phone
 - Fax
 - E-mail
 - Comments
- MS Access database:**
 - File listing database
- List File Properties:** - List File Properties -
 - Investigator
 - Agency
 - Address
 - Phone
 - Fax
 - E-mail
 - Comments
- Bookmarks:** - None -
 - Rahul
 - RD NATIONAL COLLEGE
 - rd national college sv road
 - 23673260
 - rahul@8398.com
- Selected Graphic Thumbnails:** - None -
 - Comments

AccessData Forensic Toolkit®

- File Overview

File Overview

6/26/2024

Evidence Items
Evidence Items: 1

File Items
Total File Items: 5,000
Flagged Thumbnails: 0
Other Thumbnails: 1,598

File Status
KFF Alert Files: 0
Bookmarked Items: 0
Bad Extension: 2
Empty Files: 0
From E-mail: 0
Deleted Files: 4,785
From Recycle Bin: 0
Duplicate Items: 48
OLE Subitems: 1,393
Flagged Ignore: 0
KFF Ignorable: 0
Data Carved Files: 0

File Category
Documents: 107
Spreadsheets: 0
Databases: 0
Graphics: 1,598
Multimedia: 0
E-mail Messages: 0
Executables: 105
Archives: 129
Folders: 38
Slack/Free Space: 16
Other Known Type: 24
Unknown Type: 2,983

6/26/2024 10:52:51 AM -- FTK Version 1.81.0 build 08.09.25
FTK Exec Path: C:\Program Files (x86)\AccessData\AccessData Forensic Toolkit 1.81.0\program\ftk.exe
Examiner's Machine:
Phys Mem: Total: 2,147,483,647 Available: 2,147,483,647 Used: 0
Virt Mem: Total: 2,147,352,576 Available: 1,422,921,728 Used: 724,430,848
Page File Available: 4,294,967,295

6/26/2024 10:52:51 AM -- KFF database being used: none
6/26/2024 10:52:51 AM -- Examiner's Local Machine Setting is time zone used for file times (create, modify, accessed) in file display and reports.
6/26/2024 10:52:51 AM -- New case started by Investigator Rahul using FTK version 1.81.0 build 08.09.25
Case Name: 001-2024
Case Number: 001
Case Folder: C:\Users\ITPc No. 2\Desktop\CyberForensic\001-2024
Description: CyberForensic Investigation
Case Log Options (NOT Case Reviewer Logging Options):
Log case and evidence events: Yes
Log error messages: Yes
Log bookmarking events: Yes
Log searching events: Yes
Log special searching events: Yes
Log other events: Yes
Log extended information: No
Processes to be performed:
File Extraction: Yes
File Identification: Yes
MD5 Hash: Yes
SHA1 Hash: Yes
KFF (Known File Filter): Yes
Entropy Test: Yes
Full Text Index: Yes
Prerender Thumbnails: Yes
File Listing Database: Yes
HTML File Listing: Yes
Data Carving: Yes
Preprocess Registry Files: Yes
Decrypt EFS Files: Yes
Default Case Refinement Settings:
Add files only if they satisfy BOTH the file status and the file type criteria as follows:
File Status Criteria:
Deletion status: any
Encryption status: any

AccessData File List

Case Name: 001-2024
Case number: 001
Case description: CyberForensic Investigation
Investigator: Rahul

Date: June 26, 2024
12:26:14 India Standard Time

evidence 1\FAT32-NTFS	File Name	Cr Date	Mod Date	Acc Date
\$MFT		10/3/2023 10:03:39 AM	10/3/2023 10:03:39 AM	10/3/2023 10:03:39 AM
File Type:	Unknown File Type			
Category:	Unknown			
L-size:	1835008			
Del:				
KFF:				
MD5:	3C9A31D4BA9AE1FAC09AA89509CCB05D			
\$MFTMirr		10/3/2023 10:03:39 AM	10/3/2023 10:03:39 AM	10/3/2023 10:03:39 AM
File Type:	Unknown File Type			
Category:	Unknown			
L-size:	4096			
Del:				
KFF:				
MD5:	E505EFE9D026D9163DF4ECFE28253DAD			
LogFile_1		10/3/2023 10:03:39 AM	10/3/2023 10:03:39 AM	10/3/2023 10:03:39 AM
File Type:	Unknown File Type			
Category:	Unknown			
L-size:	26214400			

- Evidence List

Evidence List

6/26/2024

Display Name: evidence 1\FAT32-NTFS
Evidence File Name: evidence 1.dd
Evidence Path: C:\Users\ITPC\No. 2\Documents\Cyber Forensic\prac2
Identification Name/Number:
Evidence Type: NTFS
Added: 6/26/2024 10:52:51 AM
Children: 3,164
Descendants: 5,000

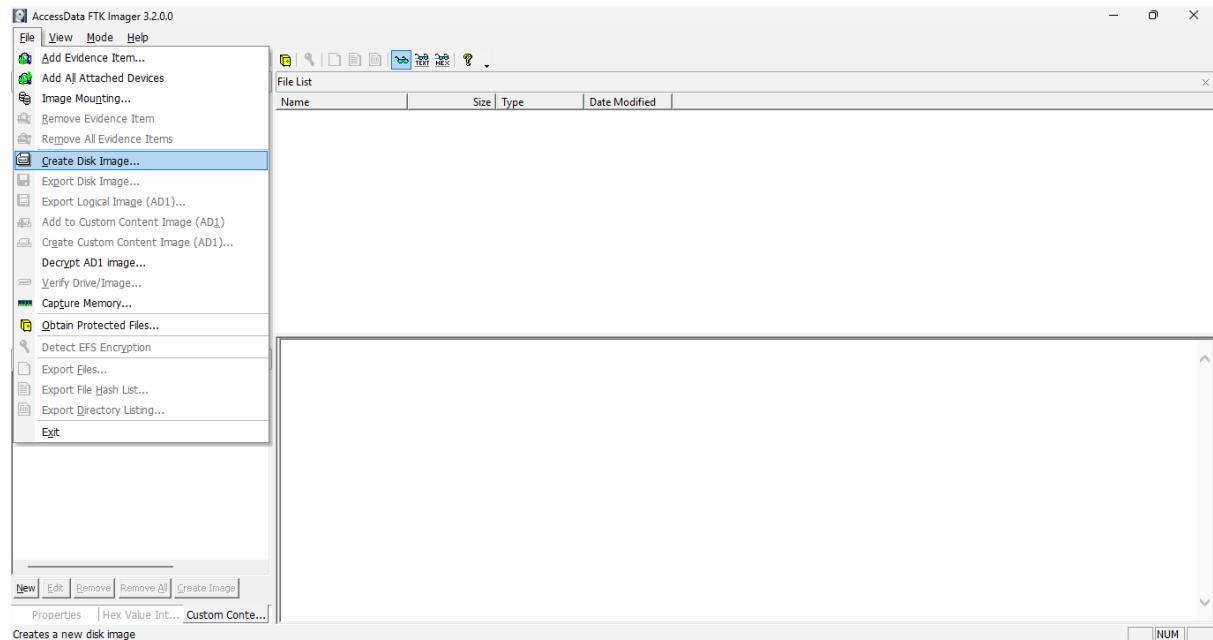
Practical: 3

Aim: Understanding & working with the process of taking a drive image using AccessData's FTK Imager tool.

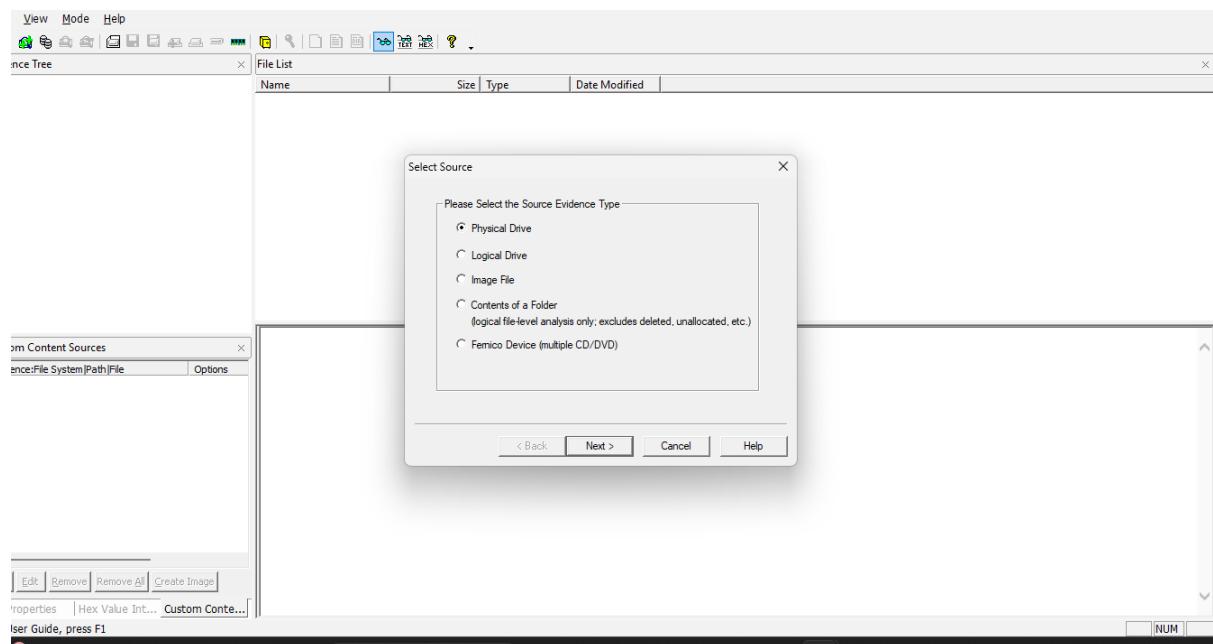
Writeup:

Step 1: Run FTK Imager.exe to start the tool

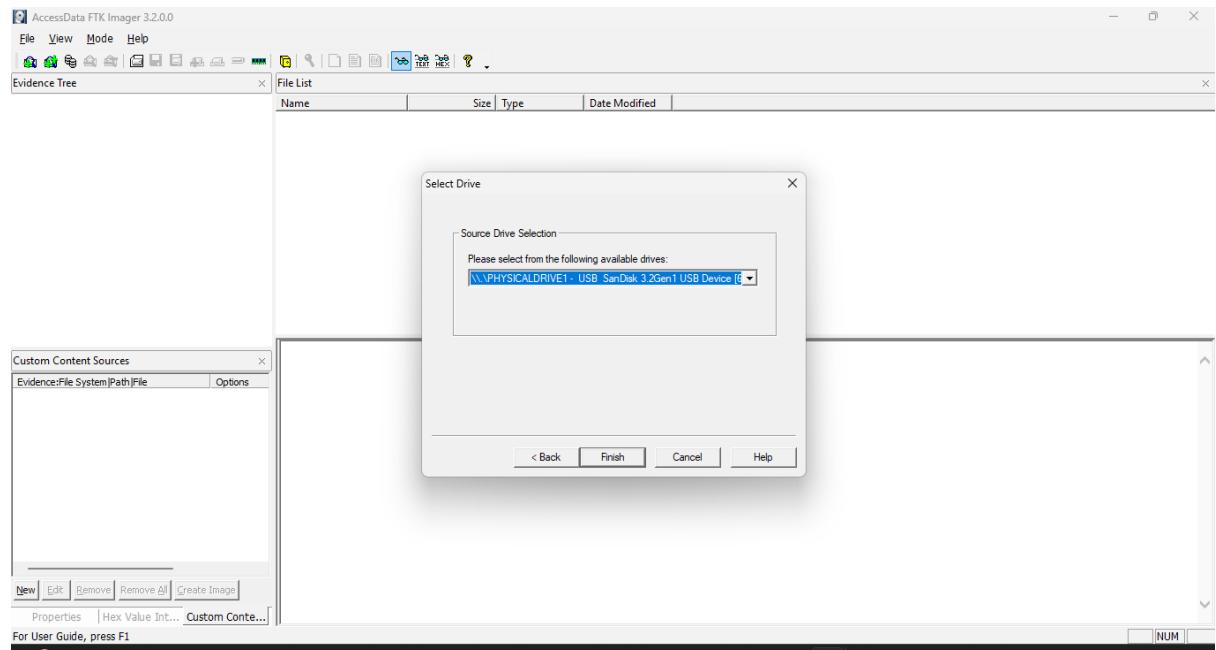
- Click on File and Select Create Disk image



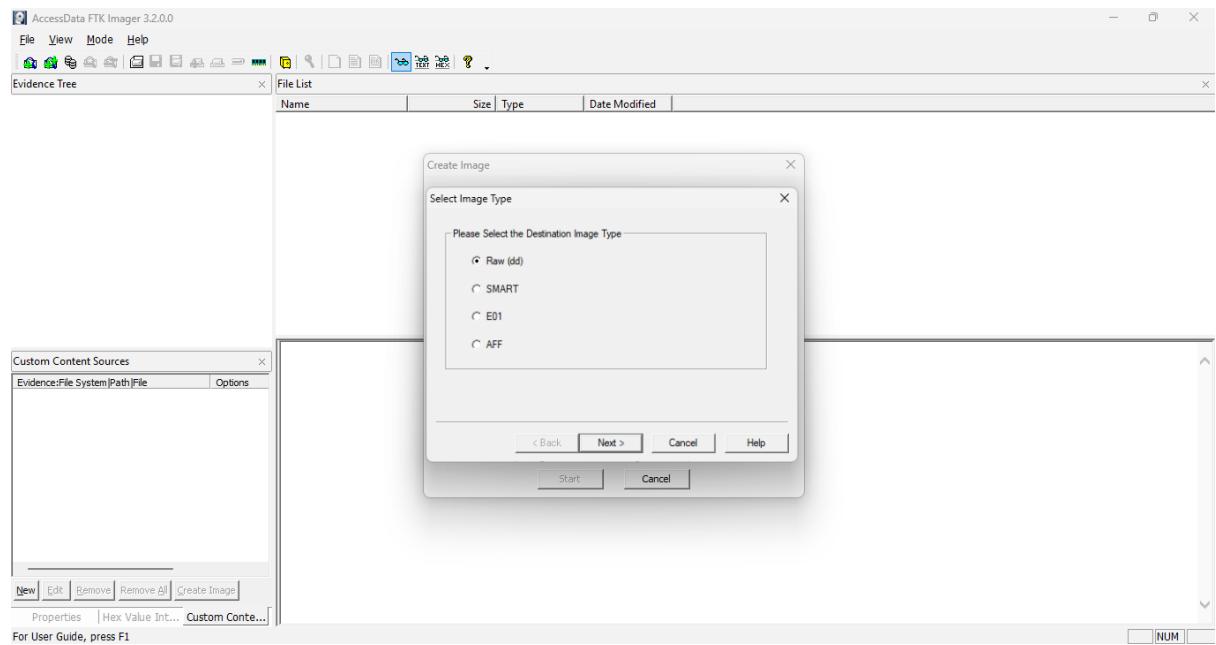
Step 2: In the Select Source dialog box, select the source you want to make an image of (Here it is Physical Drive). Click Next.



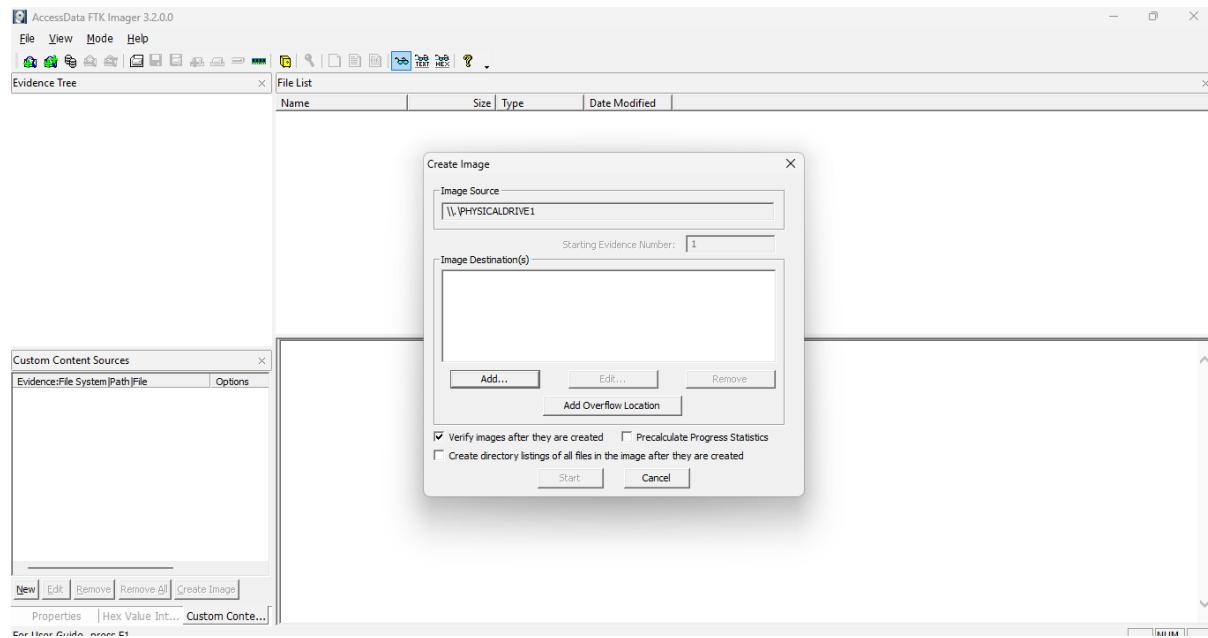
Step 3: Select the drive or browse to the source of the image you want, and then click **Finish**.



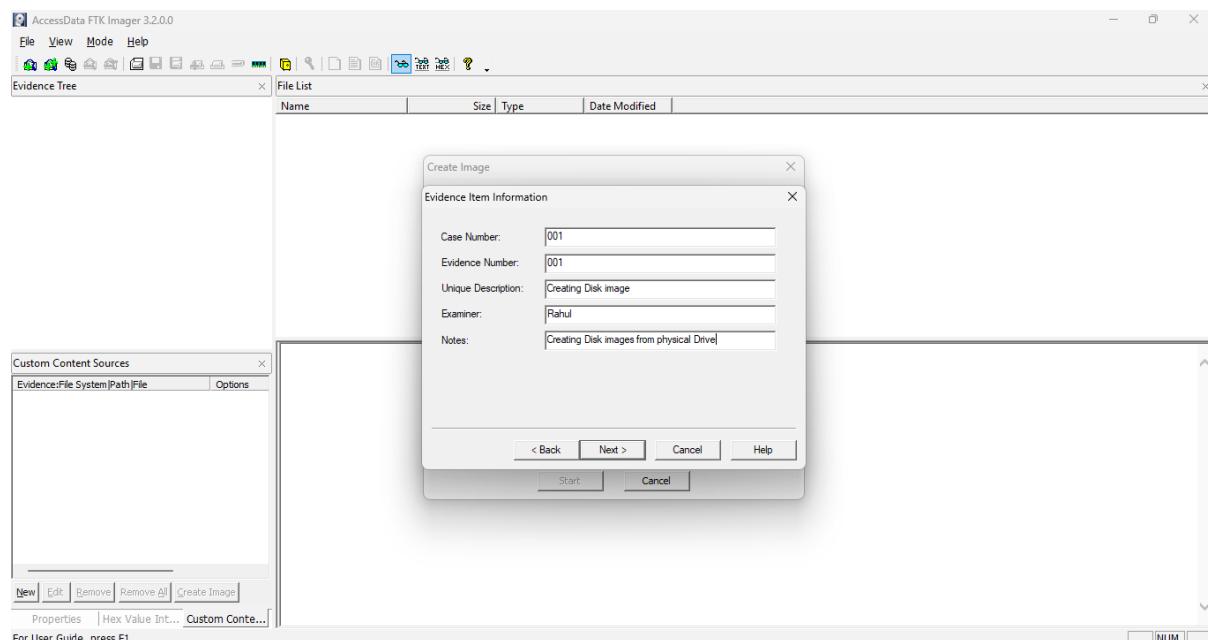
Step 4: Within Select Image Type Select Raw (dd) and Click on Next



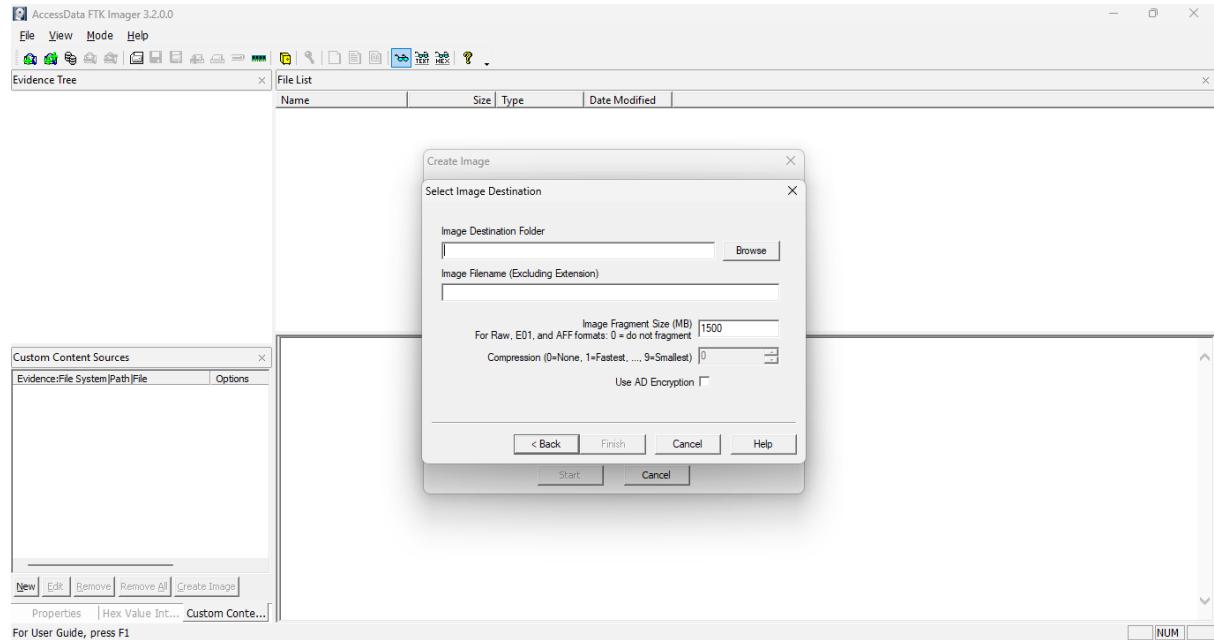
Step 5: Within Image Destination Click on Add



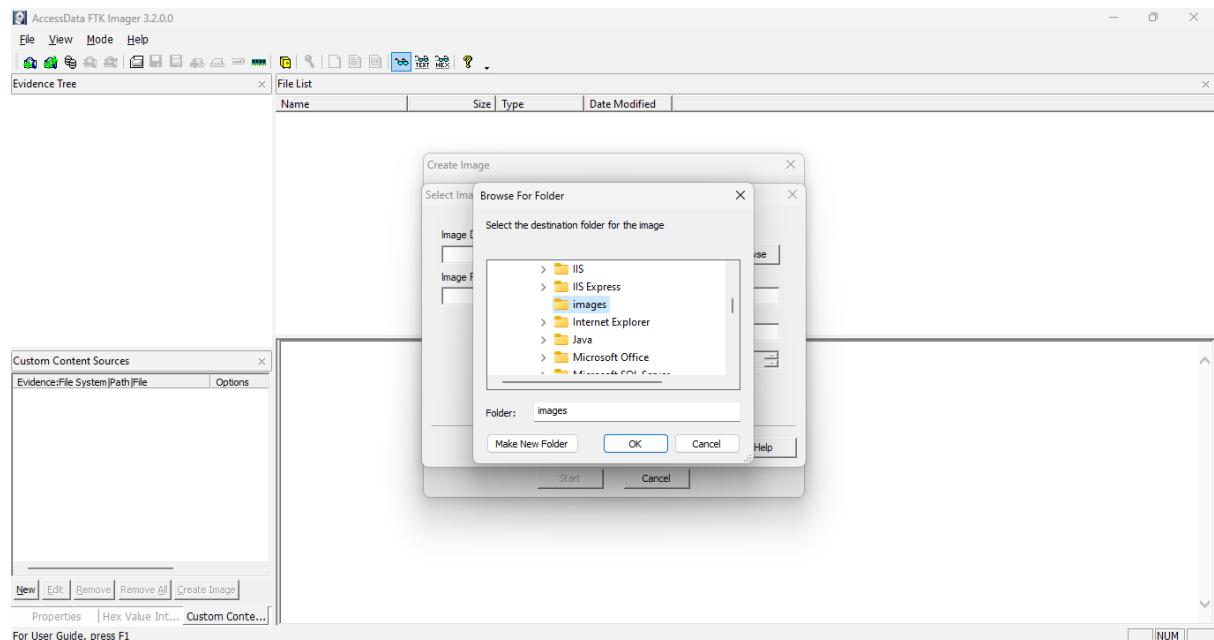
- Under **Evidence Item Information** Enter the Following Information and **Click on Next**



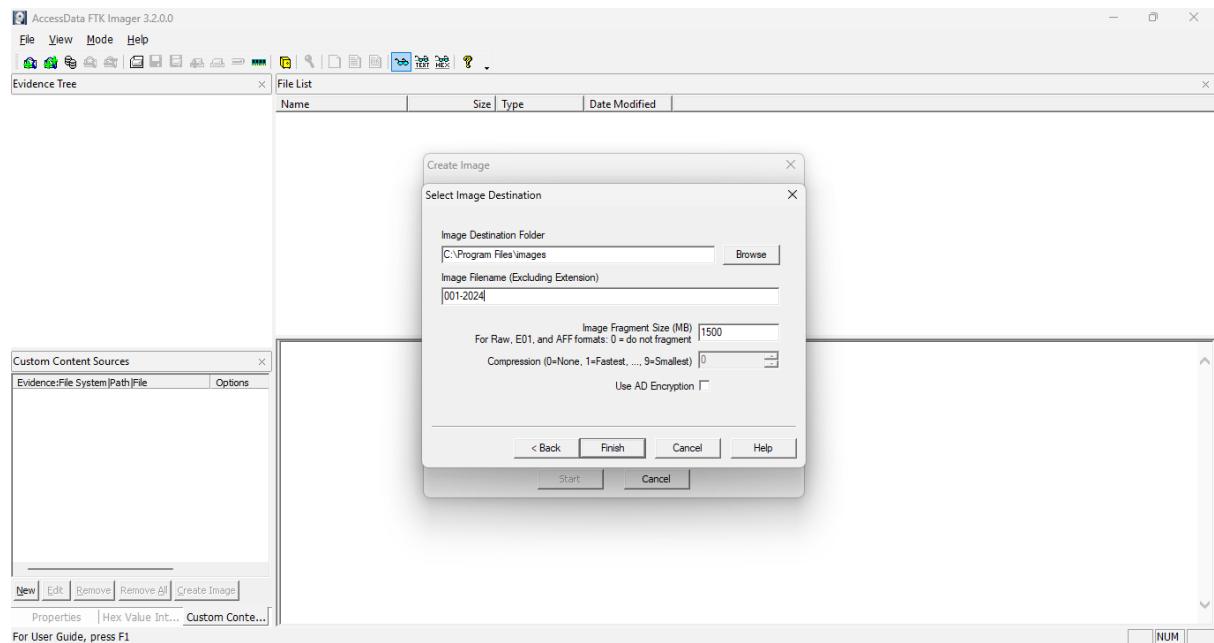
- Within Image Destination Folder Click on Browse



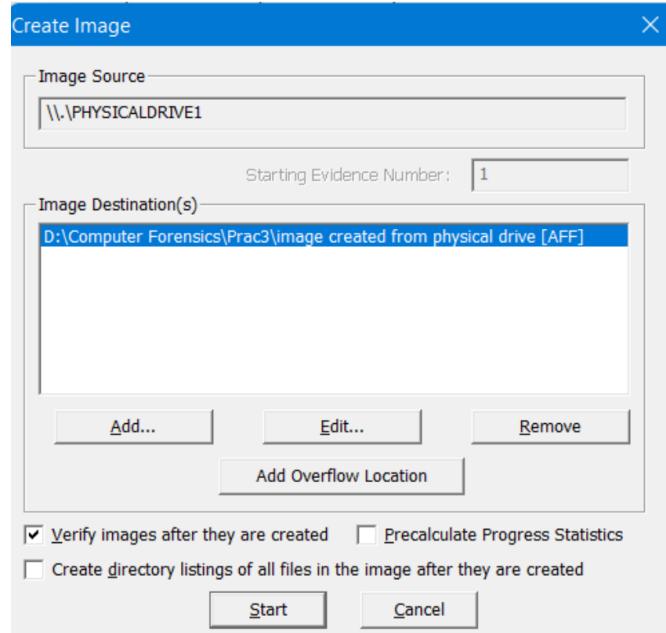
- Within Select the destination folder for the image Select images folder and click on OK



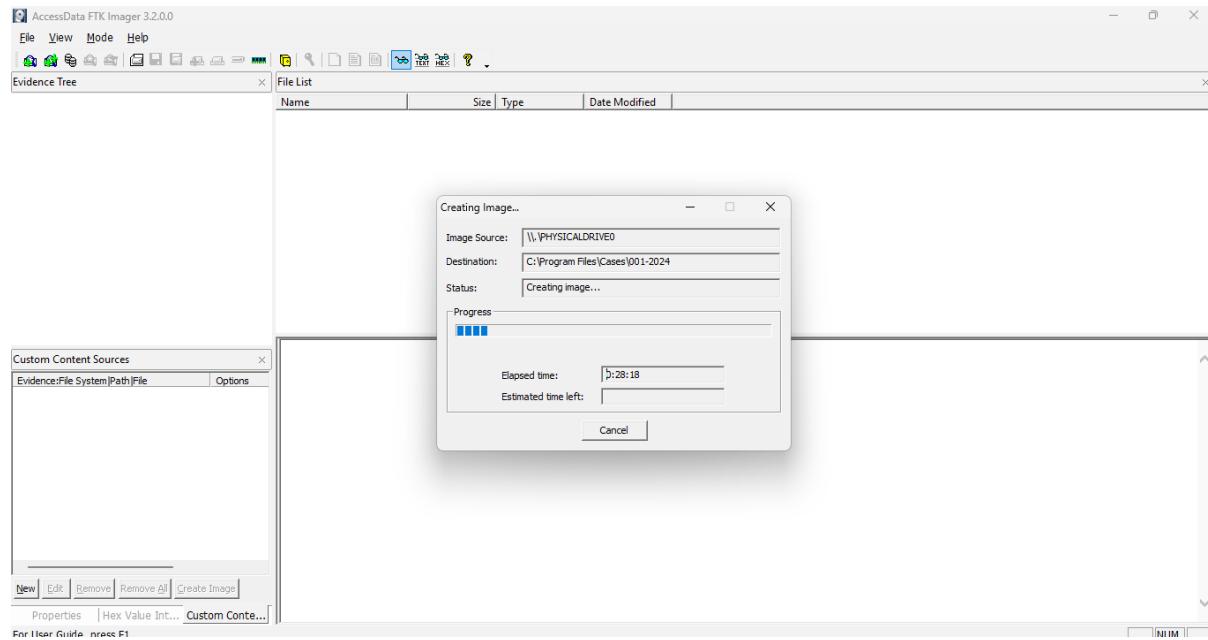
- Type Image Filename Here it is 001-2024 and Click on Finish



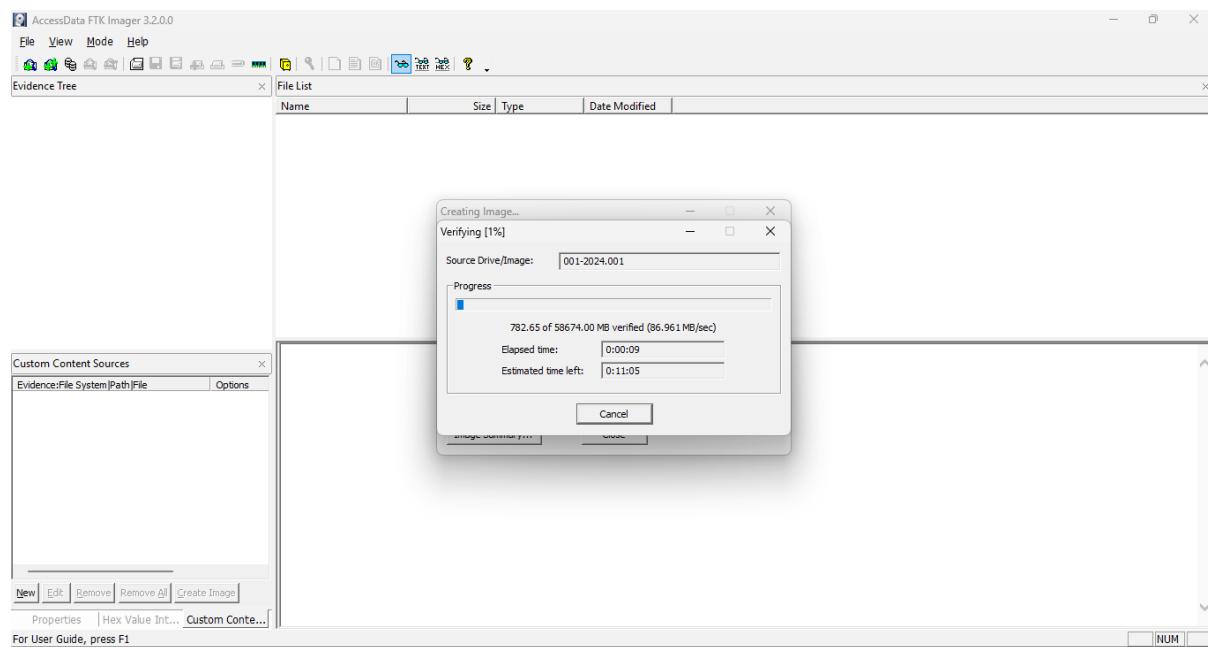
- Click Start to begin the imaging process.



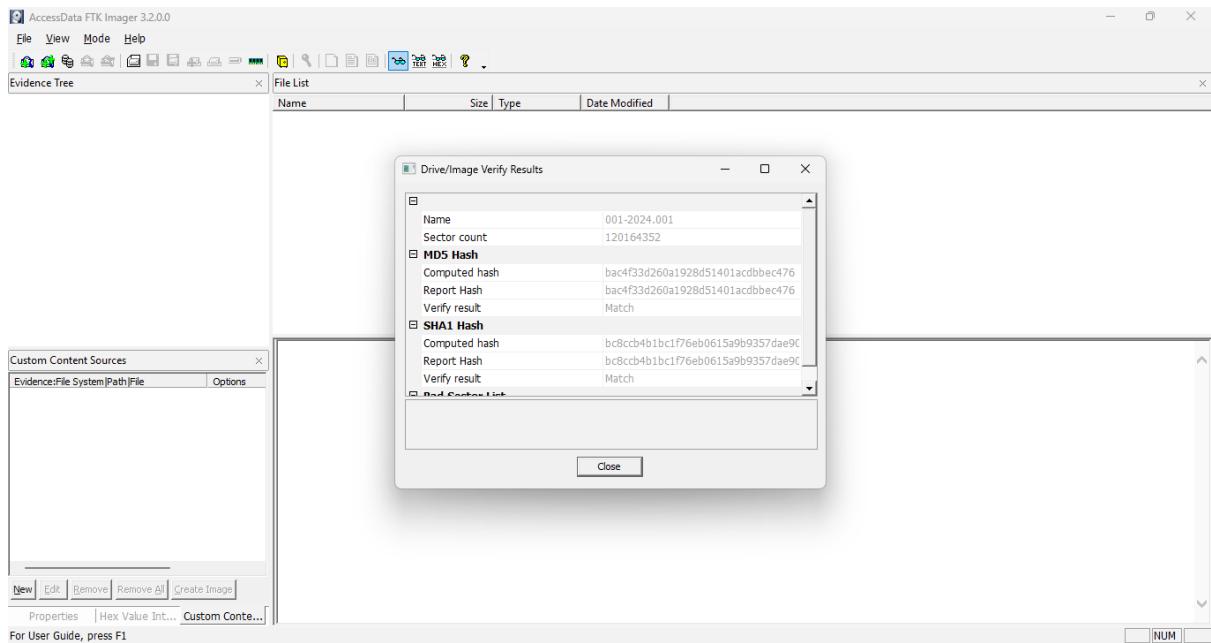
- Image Creation Process Start



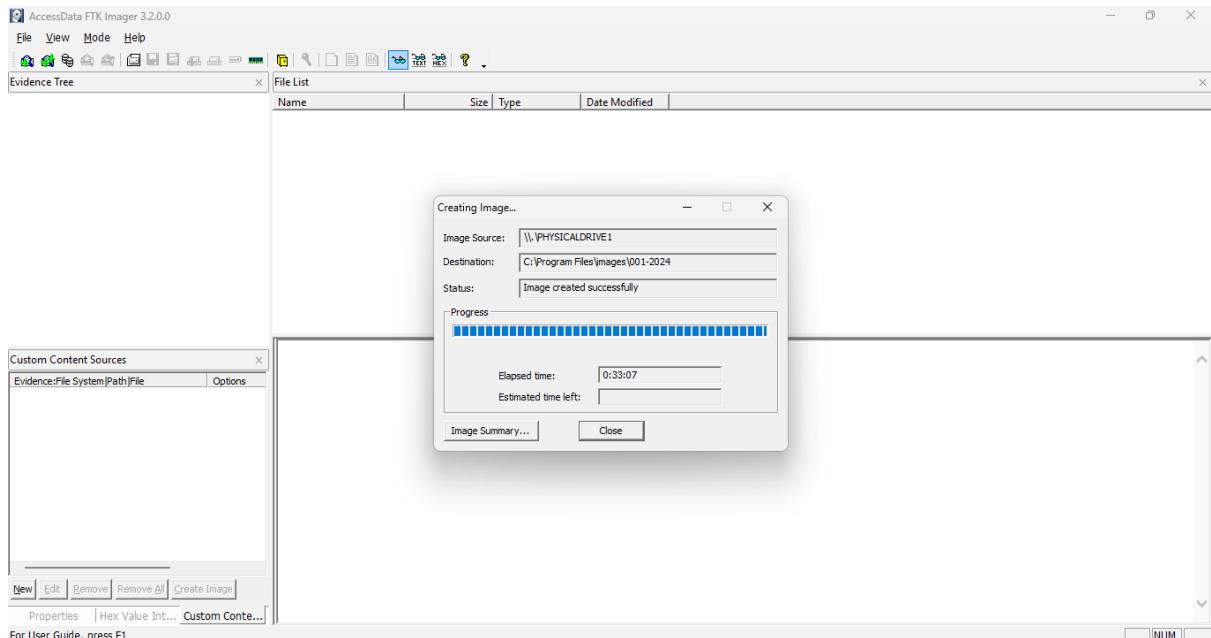
- After the images are successfully created, the Drive/Image Verify Results box shows detailed image information, including MD5 and SHA1 check sums, and bad sectors



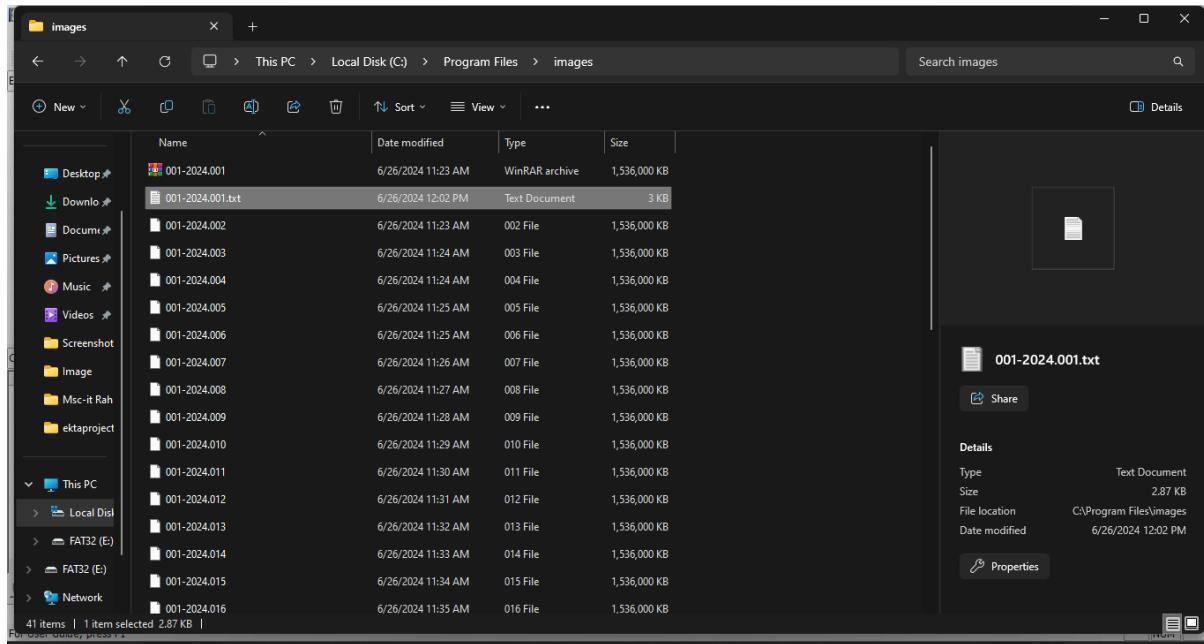
- Once the acquisition is complete, you can view an image summary and the drive will appear in the evidence list in the left hand side of the main FTK Imager window. You can right-click on the drive name to Verify the Image



- Image Created Successfully**



Step 6: After Creation of Image of One text document created (Here it is 001-2024.txt). it give image information



```

001-2024.001.txt      001-2024.001.txt
File   Edit   View
Created By AccessData® FTK® Imager 3.2.0.0

Case Information:
Acquired using: ADI3.2.0.0
Case Number: 001
Evidence Number: 001
Unique description: creating disk image
Examiner: rahul
Notes: creating disk image

-----
Information for C:\Program Files\Images\001-2024:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 7,479
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 120,164,352
[Physical Drive Information]
Drive Model: USB SanDisk 3.2Gen1 USB Device
Drive Serial Number: 0491d8195cb275b53004
Drive Interface Type: USB
Removable drive: True
Source data size: 58674 MB
Sector count: 120164352
[Computed Hashes]
MD5 checksum: bac4f33d260a1928d51401acdbbec476
SHA1 checksum: bc8ccb4b1bc1f76eb0615a9b9357dae9014e0518

Ln 1, Col 1    2,853 characters           100%    Windows (CRLF)    UTF-8 with BOM

```

The screenshot shows a terminal window titled "001-2024.001.txt" containing the following text:

```
C:\Program Files\images\001-2024.013
C:\Program Files\images\001-2024.014
C:\Program Files\images\001-2024.015
C:\Program Files\images\001-2024.016
C:\Program Files\images\001-2024.017
C:\Program Files\images\001-2024.018
C:\Program Files\images\001-2024.019
C:\Program Files\images\001-2024.020
C:\Program Files\images\001-2024.021
C:\Program Files\images\001-2024.022
C:\Program Files\images\001-2024.023
C:\Program Files\images\001-2024.024
C:\Program Files\images\001-2024.025
C:\Program Files\images\001-2024.026
C:\Program Files\images\001-2024.027
C:\Program Files\images\001-2024.028
C:\Program Files\images\001-2024.029
C:\Program Files\images\001-2024.030
C:\Program Files\images\001-2024.031
C:\Program Files\images\001-2024.032
C:\Program Files\images\001-2024.033
C:\Program Files\images\001-2024.034
C:\Program Files\images\001-2024.035
C:\Program Files\images\001-2024.036
C:\Program Files\images\001-2024.037
C:\Program Files\images\001-2024.038
C:\Program Files\images\001-2024.039
C:\Program Files\images\001-2024.040

Image Verification Results:
Verification started: Wed Jun 26 11:55:59 2024
Verification finished: Wed Jun 26 12:02:30 2024
MD5 checksum: bac4f33d260a1928d51401acdbecc476 : verified
SHA1 checksum: bc8ccb4b1bc1f76eb0615a9b9357dae9014e0518 : verified
```

At the bottom of the terminal window, the status bar displays: Ln 1, Col 1 2,853 characters | 100% Windows (CRLF) | UTF-8 with BOM.

Practical: 4

Aim: Using Wireshark Tool.

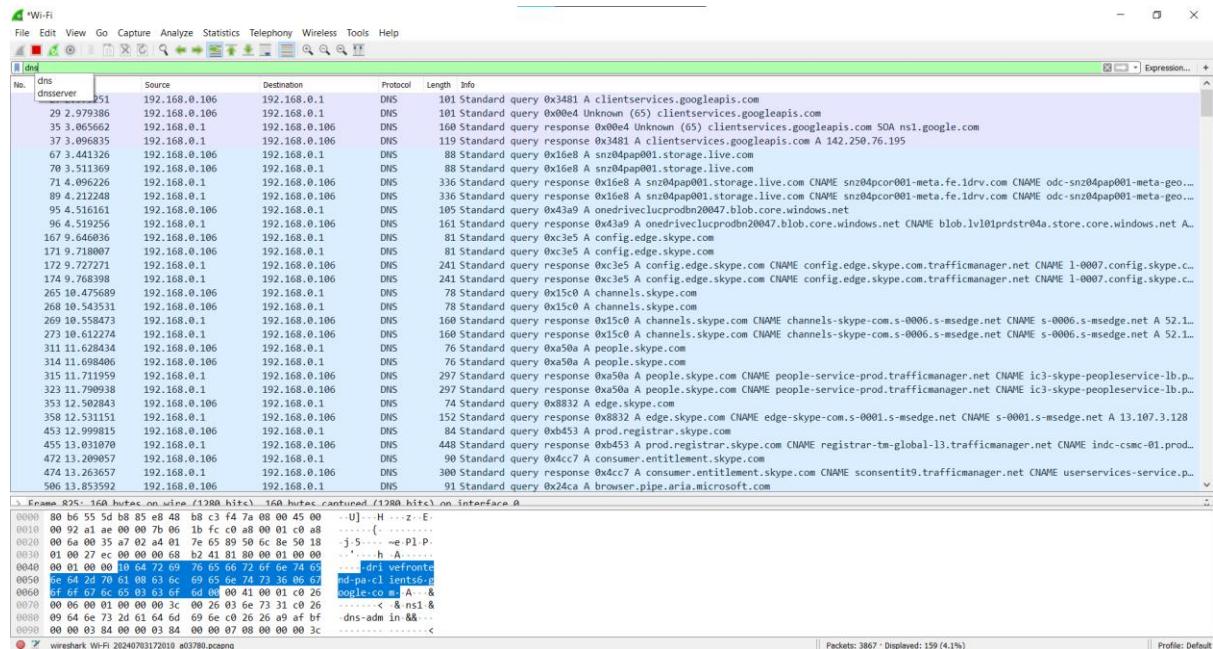
Writeup:

Wireshark is a network packet analyzer that intercepts, captures and logs information about packets passing through a network interface. This is useful for analyzing network problems, detecting network intrusions, network misuse, and other security problems, monitor usage and gather statistics, and many other applications.

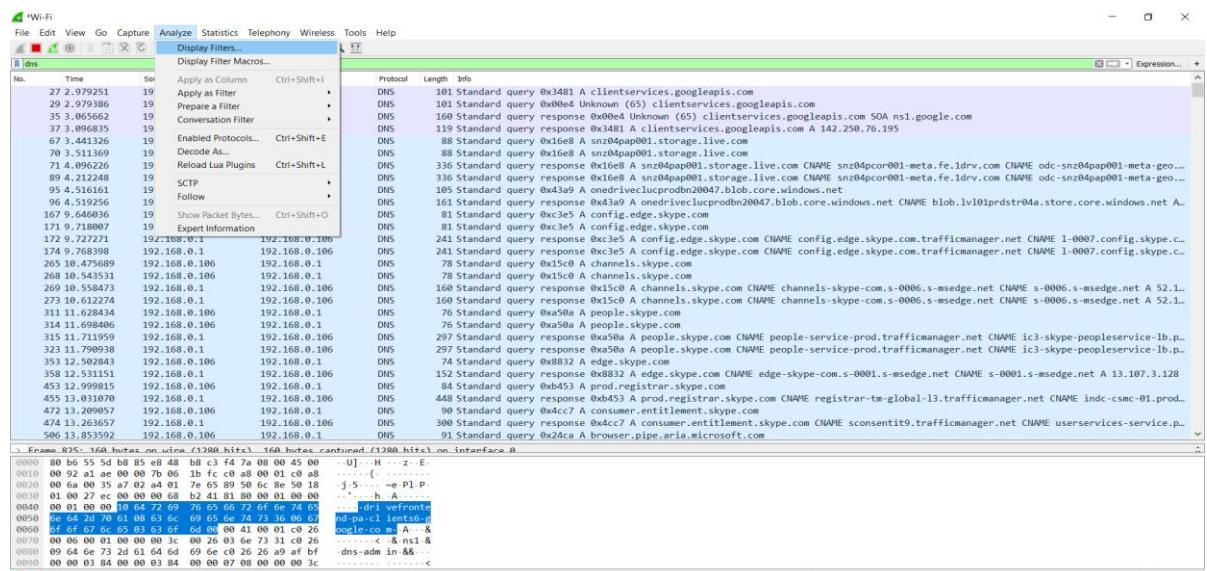
Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount, of packets to sift through. That's where Wireshark's filters come in.

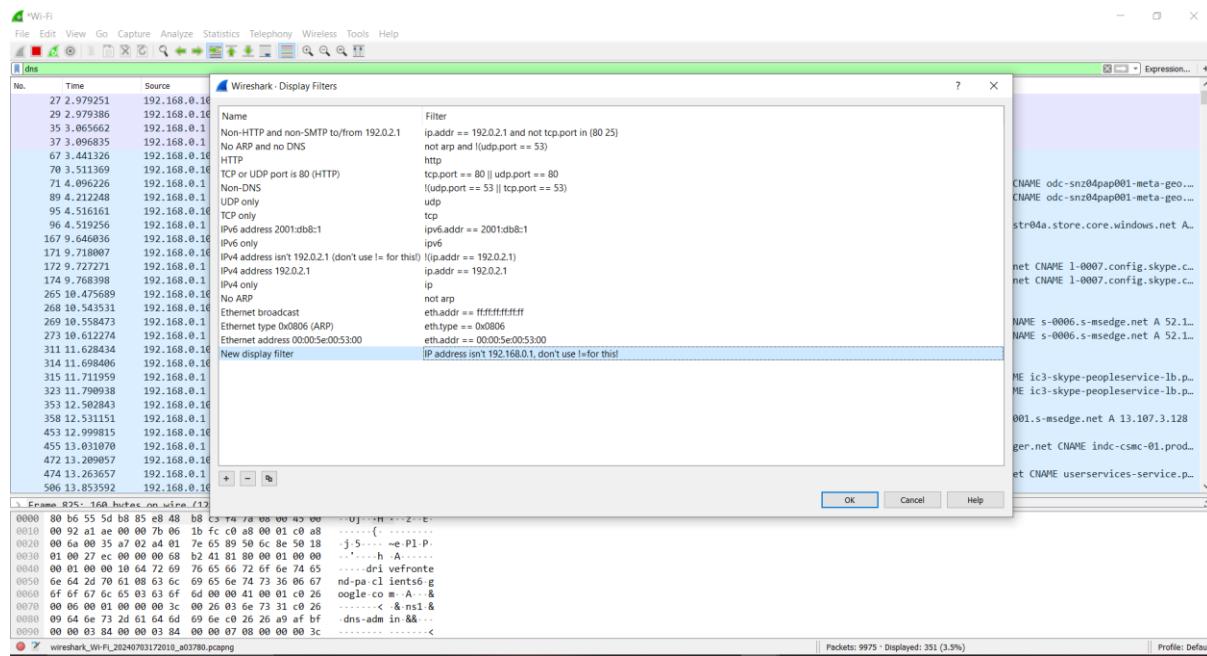
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



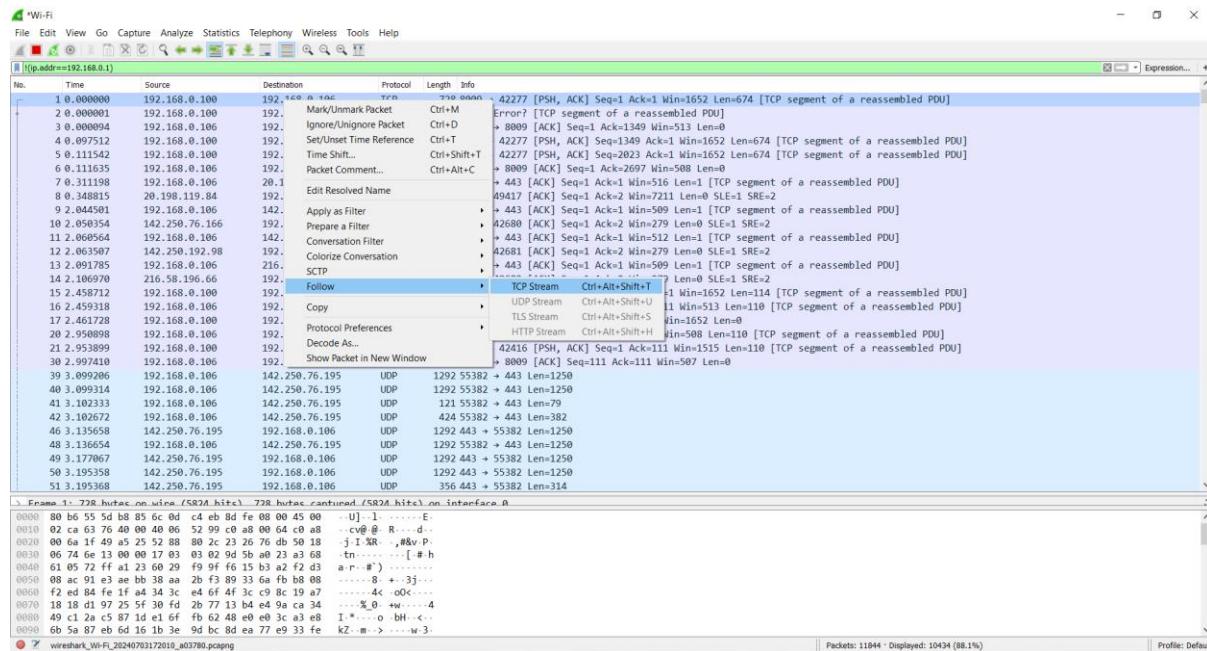
We can also click the Analyze menu and select Display Filters to create a new filter



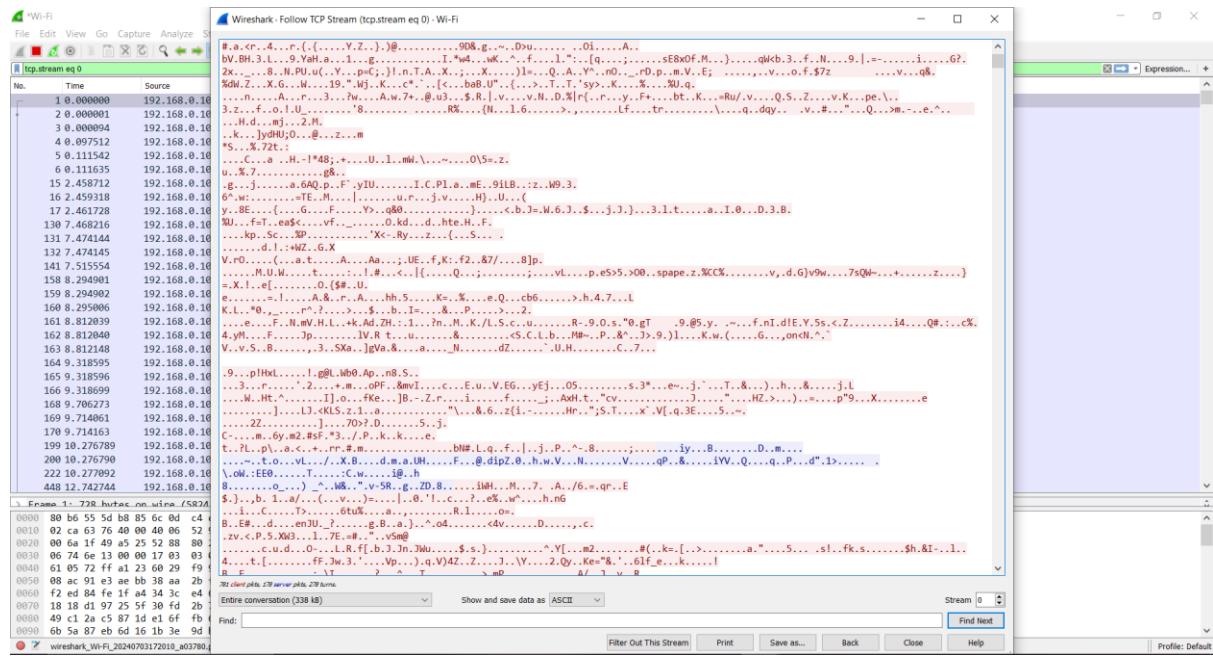
Click on OK



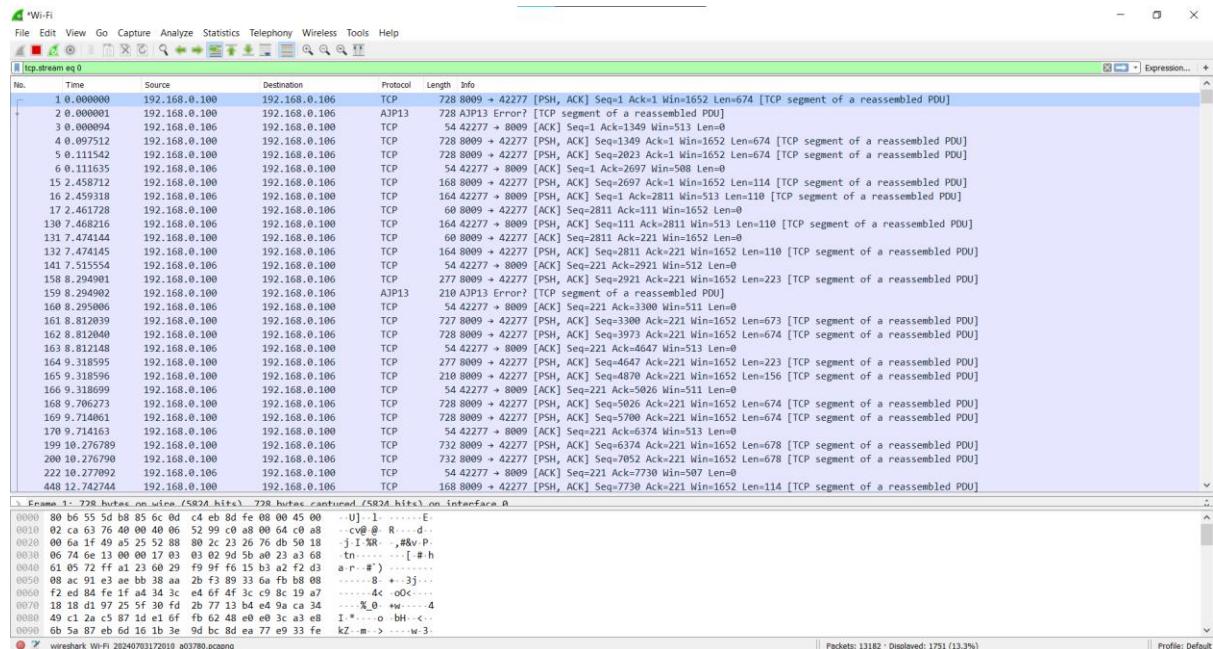
Another interesting thing you can do is right-click a packet and select Follow TCP Stream.



You'll see the full conversation between the client and the server.

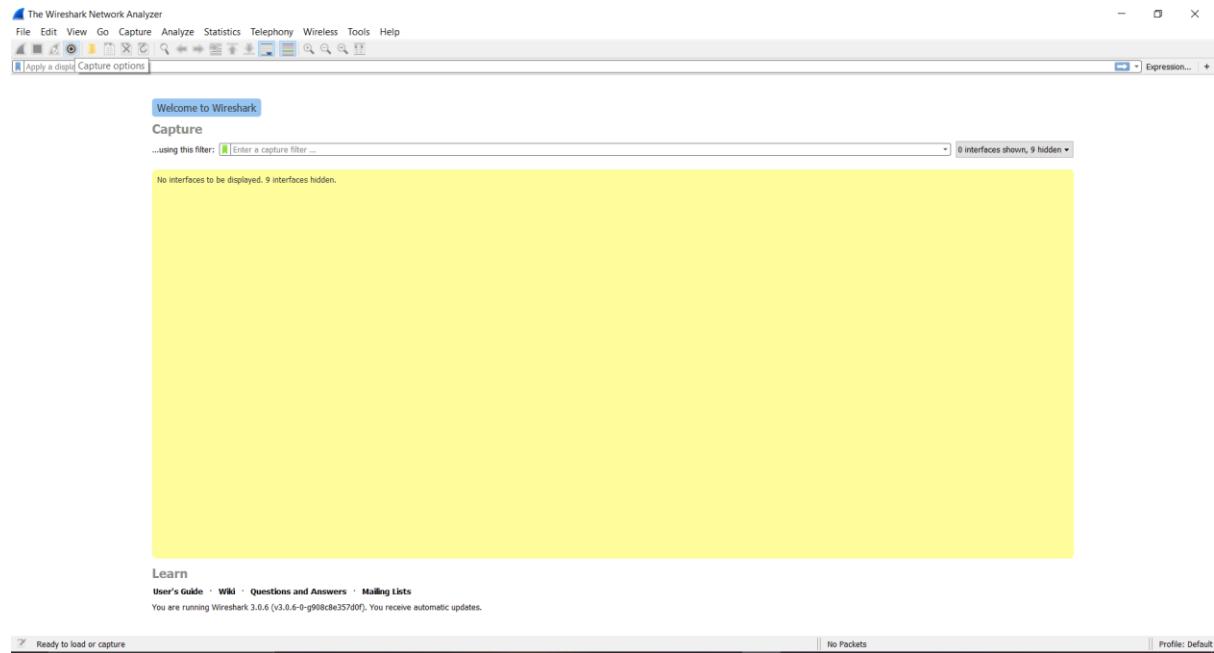


Close the window and you'll find a filter has been applied automatically — Wireshark is showing you the packets that make up the conversation

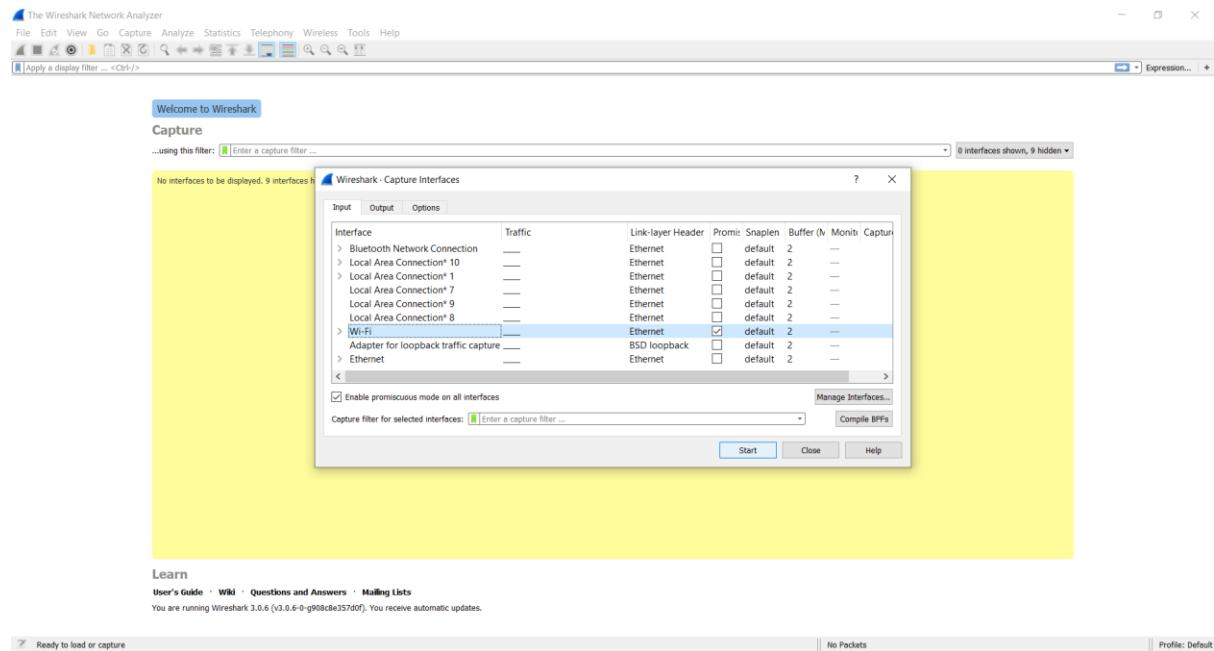


Step 1: Exploring Wireshark

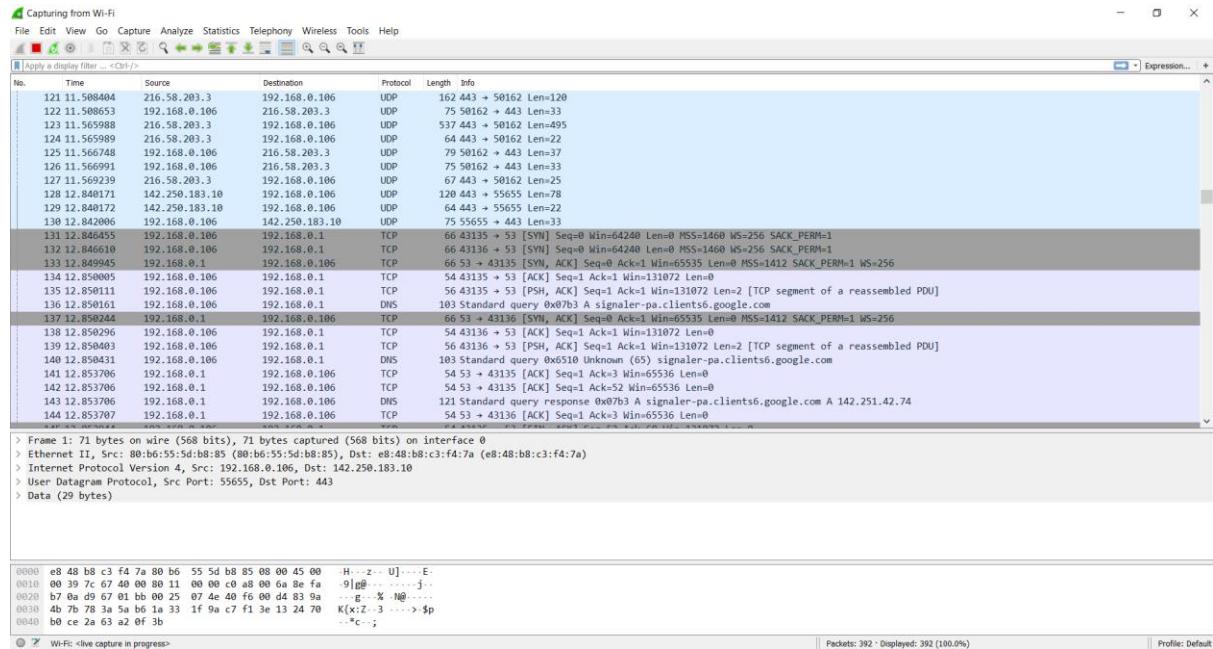
- On menu bar select Capture Option



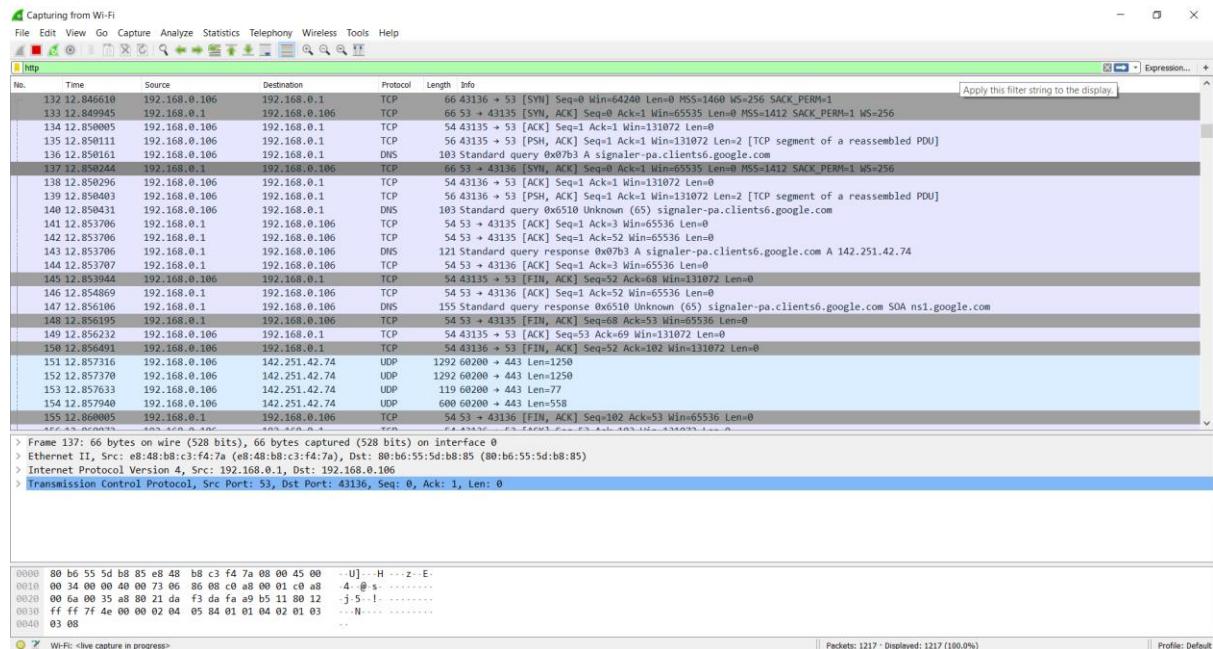
- Select Once you click on start



- Wireshark starts to capture the packets on that interface.

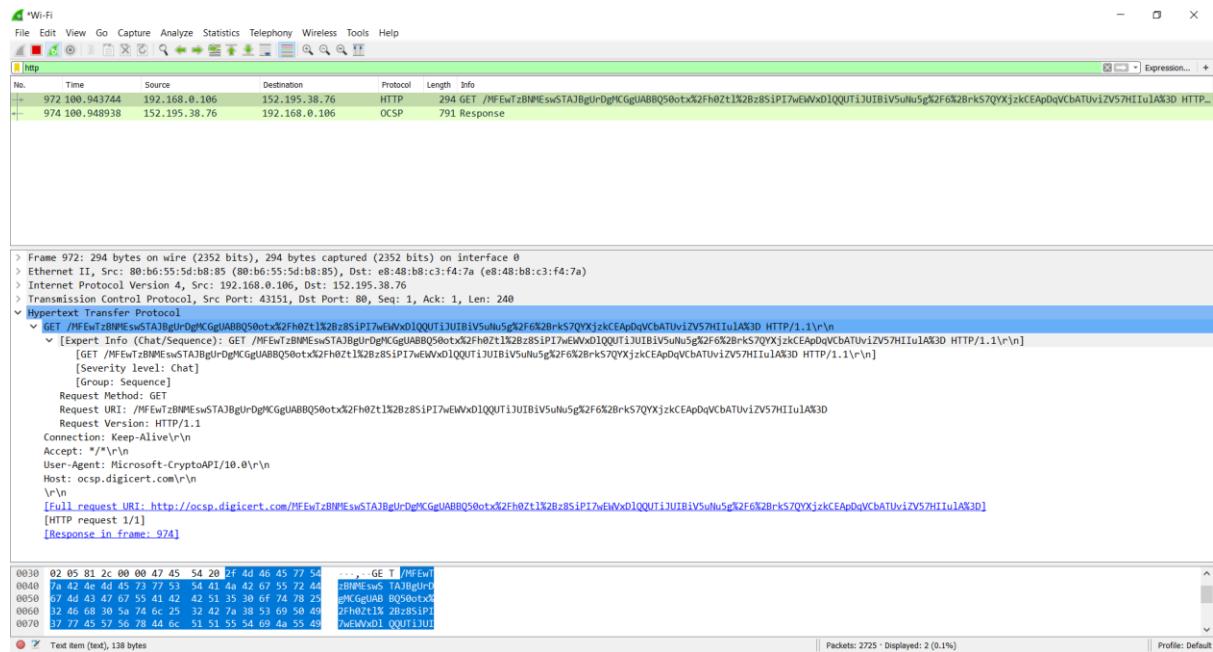


Step 2: Filter packets with HTTP protocol



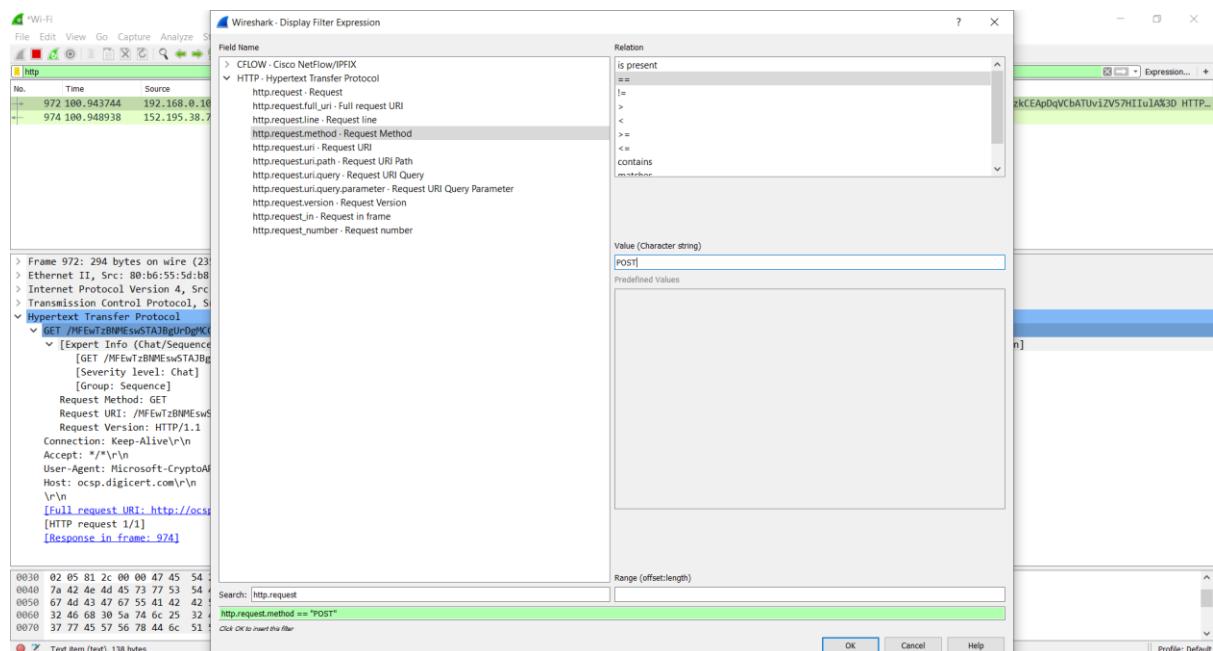
- A file with only text:

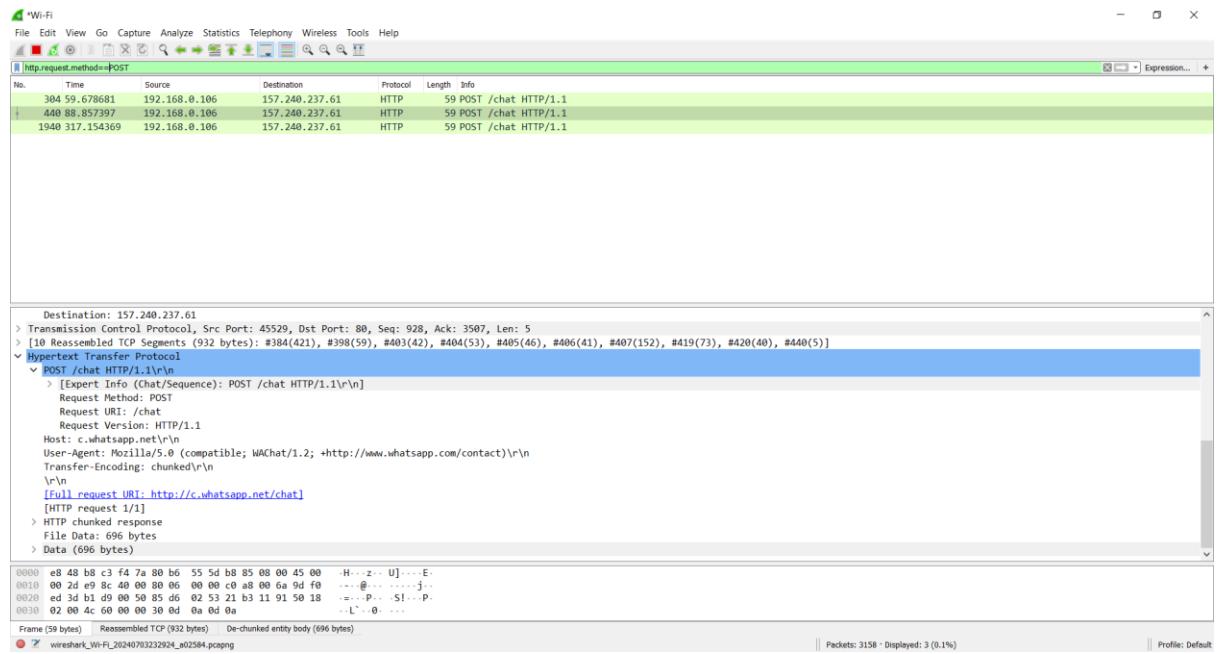
<msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?0a9109c2b28701dc>



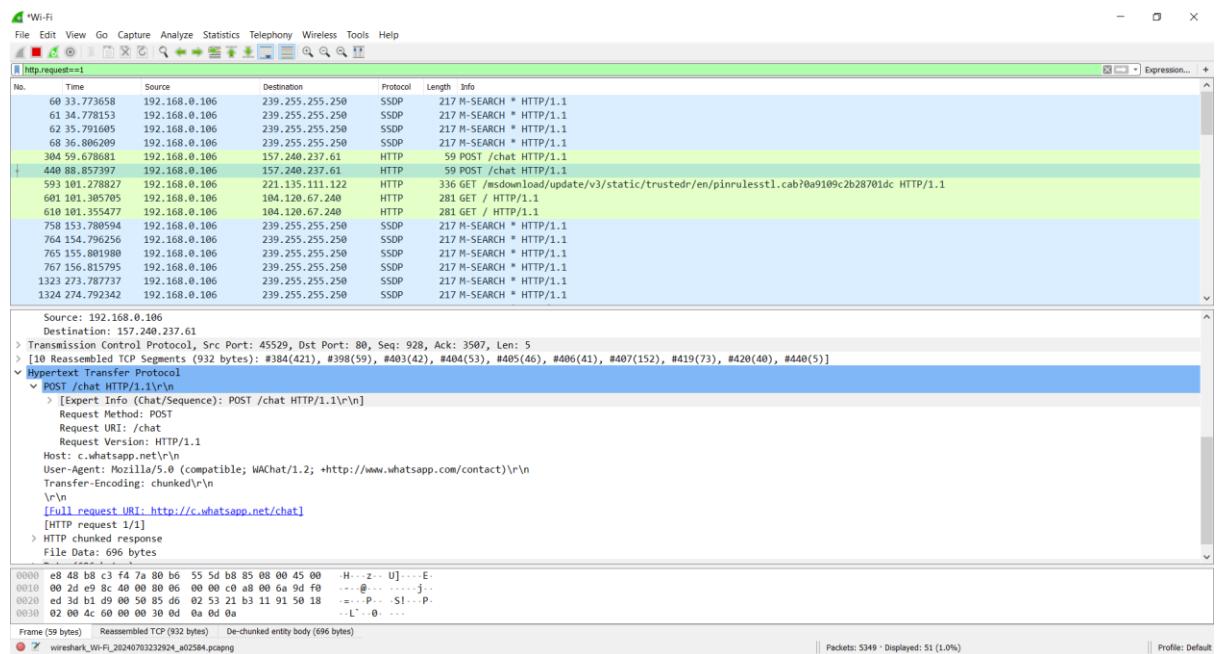
Step 3: Applying different filters using expressions.

- Filtering HTTP POST request
- Click on Expression and Select the following and Click on OK





- Filtering HTTP REQUEST==1



Practical: 5

Aim: Using Data Acquisition Tools [ProDiscover].

Writeup:

Tasks to be performed:

- Creating a New Project
- Save a project
- Preview a directly connected evidence drive
- Conducting Live Preview of a Remote Disk
- Capture an image of an attached drive
- Capturing Physical Memory
- Add an image file to a project
- Restore an Image to directly connected drive

Step 1: Creating a New Project

- Start ProDiscover and Type Project Number and Project File Name and Click on Open

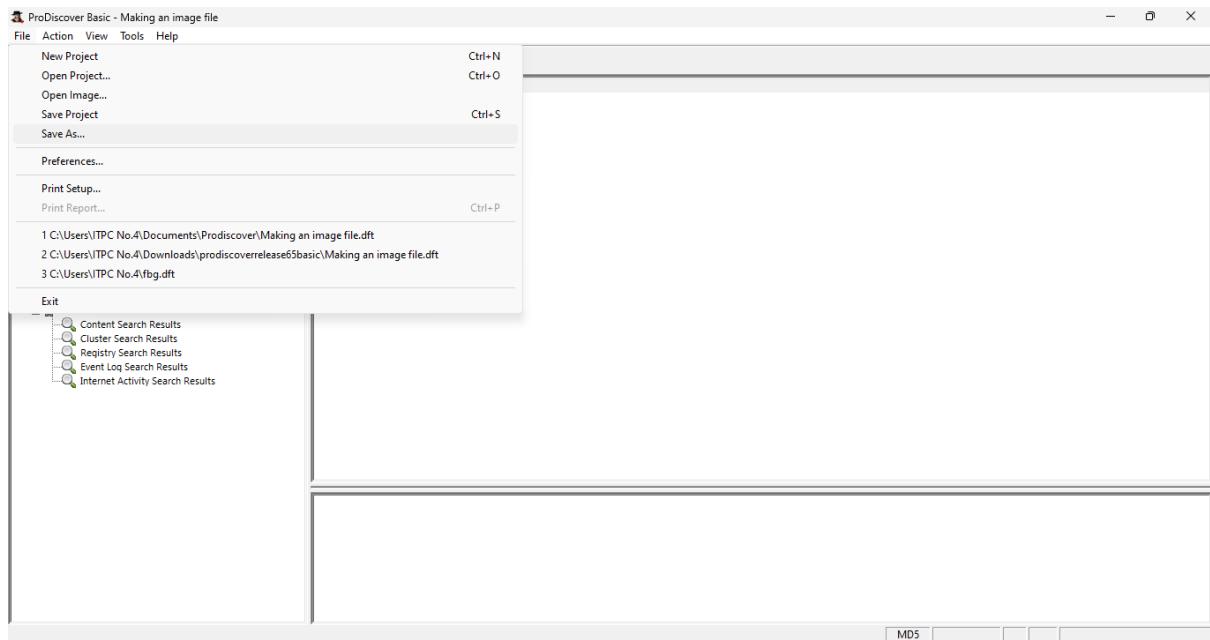


- Here We Can See ProDiscover Create New Project

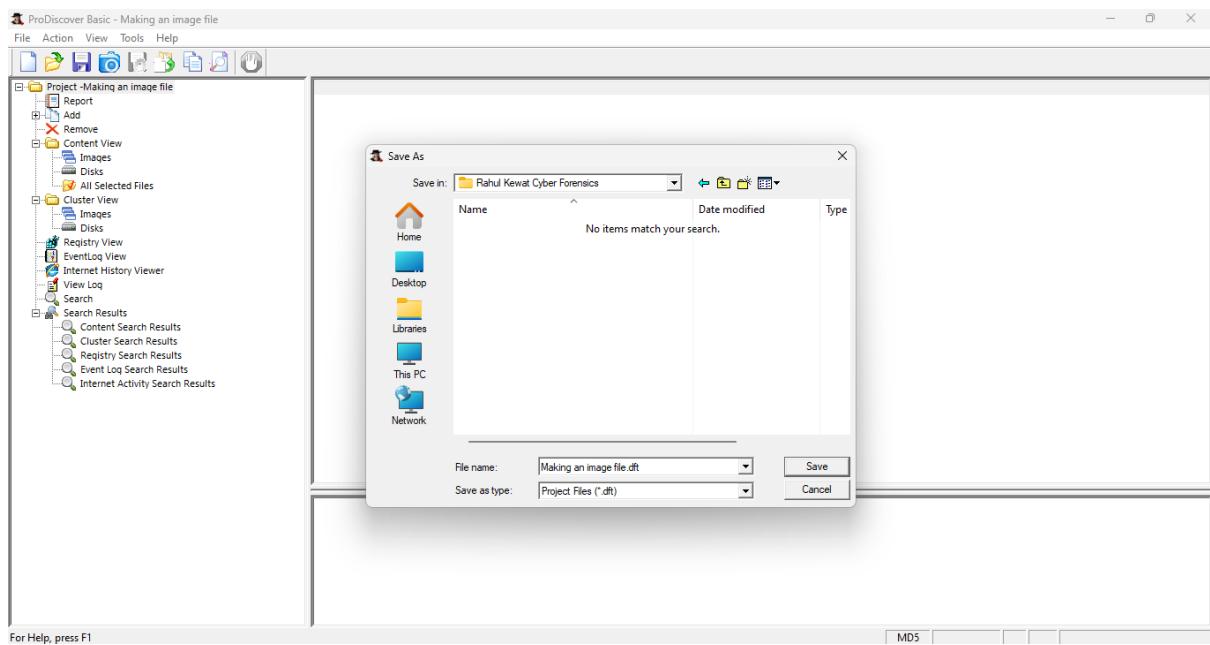


Step 2: Saving a project

- Click on File and Select Save As..



- Select the destination path and click the Save button



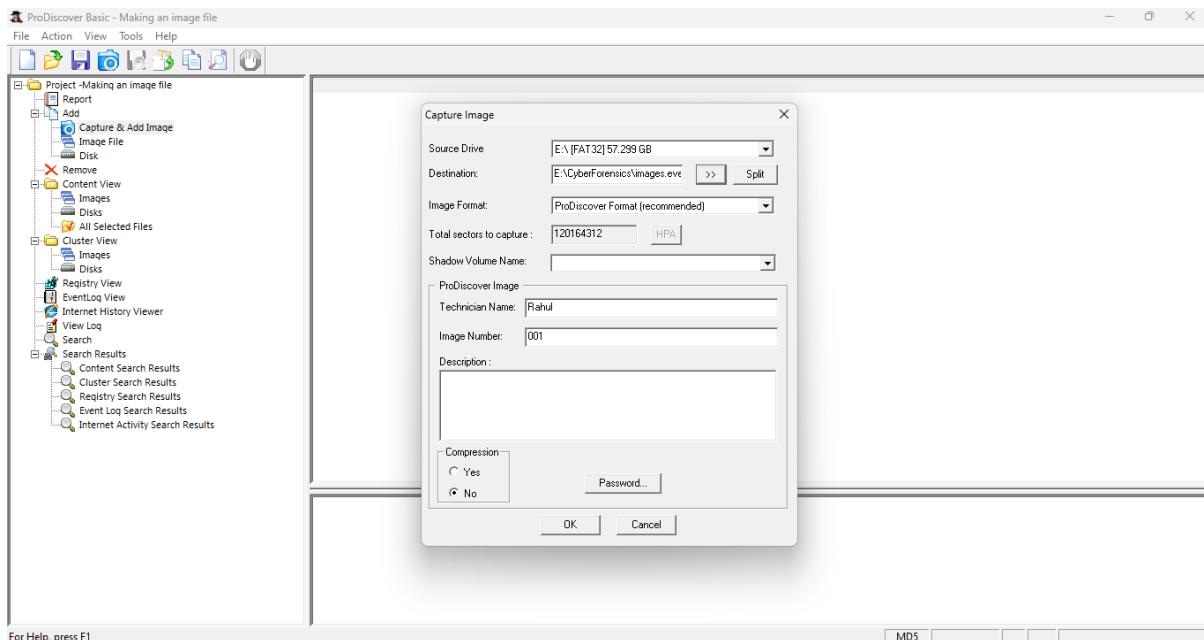
Step 3: Preview a directly connected evidence drive

- **Launch ProDiscover**
- **Select open project tab option.**
- **Select the project file to open and click Open button**
- **ProDiscover opens the project file and generates a template report in the work area**

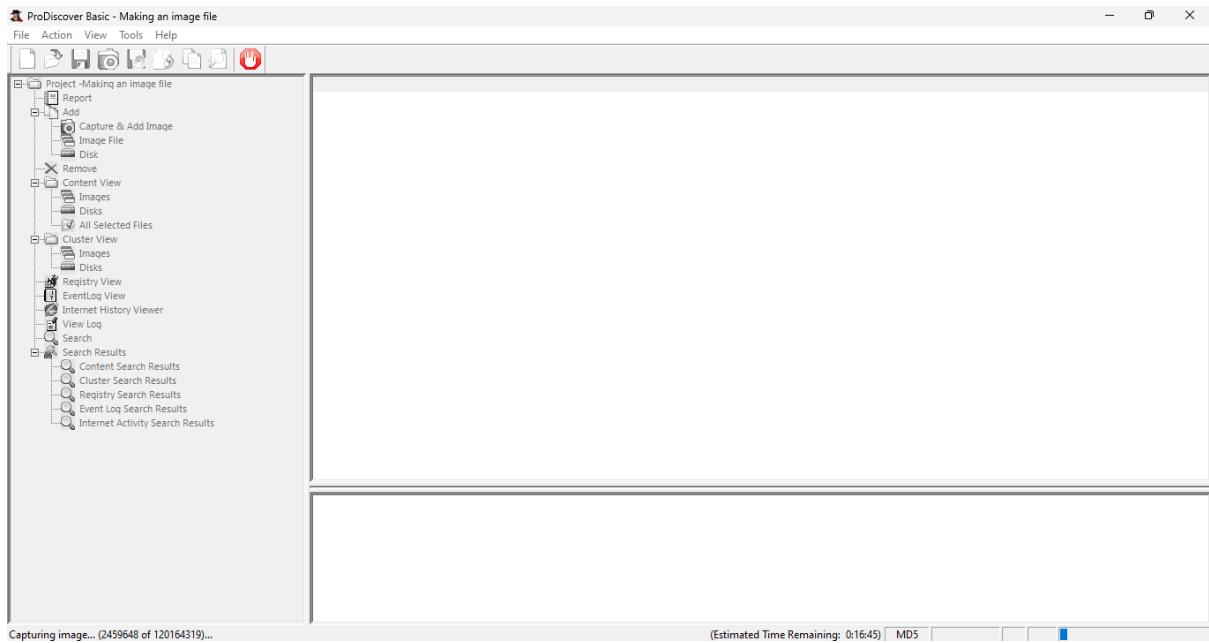


- **Under Report, expand Add and click on Capture & Add Image.**
- **Give Destination, add Technician Name and image number and click on OK**

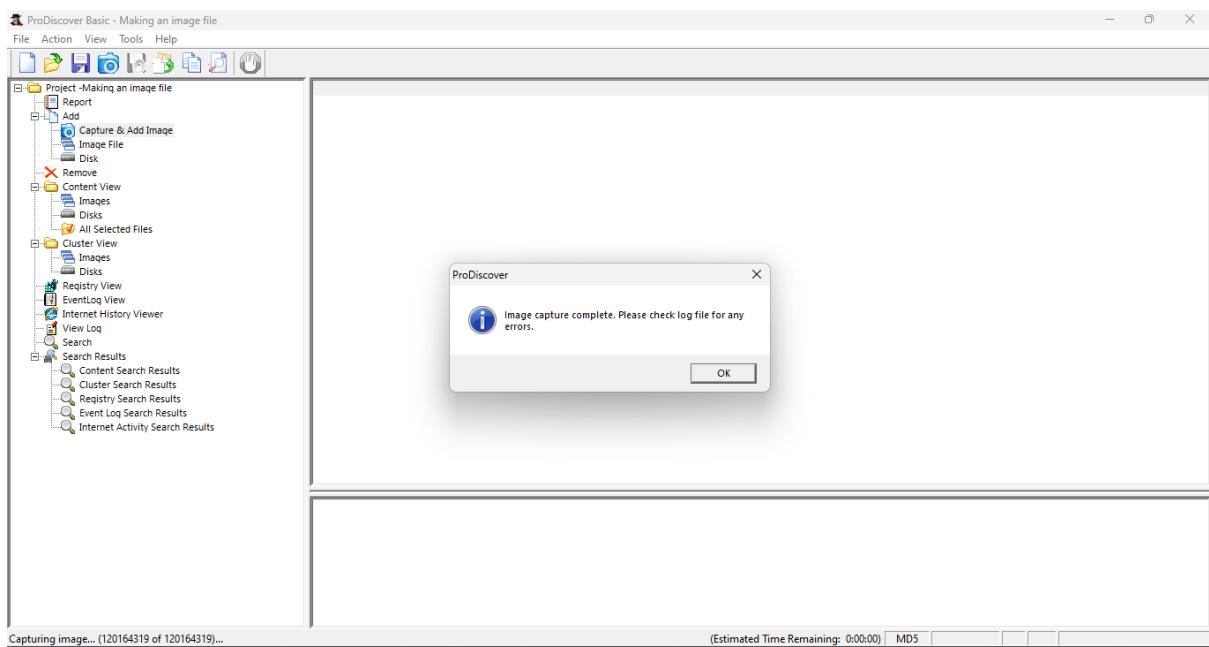
Note: Use Pen drive for Source Drive and and Create or Select File in Physical C-Drive for Destination



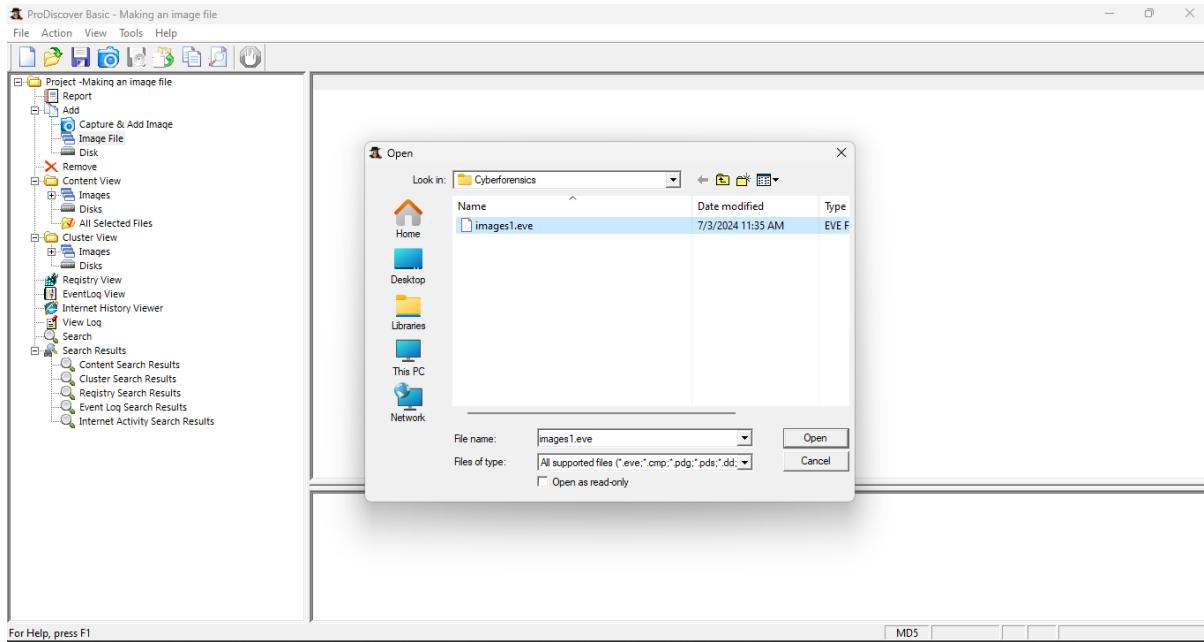
- Image Capture Process Start



- Once the **image capturing** is completed, click on **OK**



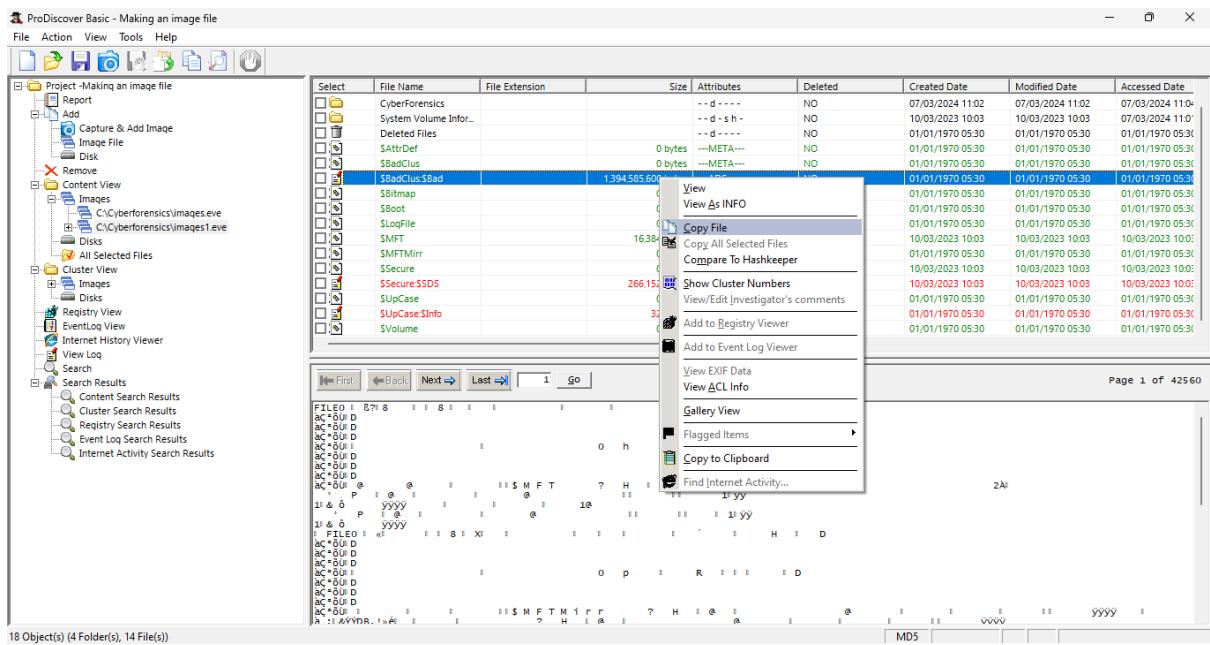
- Under Add, click on Image File, click on the image that you created and click Open



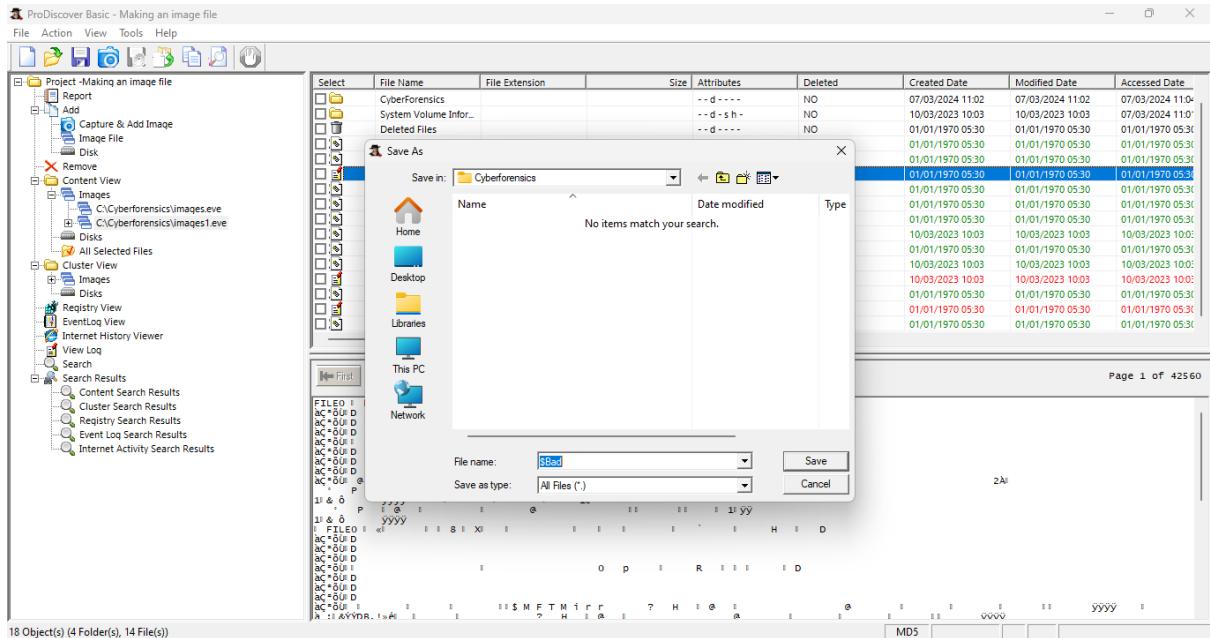
- The image file will get added. Then under Content view, click on images and select the image.

Select	File Name	File Extension	Size	Attributes	Deleted	Created Date	Modified Date	Accessed Date
□	CyberForensics			--- d ---	NO	07/03/2024 11:02	07/03/2024 11:02	07/03/2024 11:02
□	System Volume Infor...			--- d - s h -	NO	10/03/2023 10:03	10/03/2023 10:03	07/03/2024 11:02
□	Deleted Files			--- d ---	NO	01/01/1970 05:30	01/01/1970 05:30	01/01/1970 05:30
□	\$AttrDef		0 bytes	---META---	NO	01/01/1970 05:30	01/01/1970 05:30	01/01/1970 05:30
□	\$BadClus		0 bytes	---META---	NO	01/01/1970 05:30	01/01/1970 05:30	01/01/1970 05:30
□	\$BadClus\$Bad		1394585.600 bytes	---ADS---	NO	01/01/1970 05:30	01/01/1970 05:30	01/01/1970 05:30
□	\$Bitmap		0 bytes	---META---	NO	01/01/1970 05:30	01/01/1970 05:30	01/01/1970 05:30
□	\$Boot		0 bytes	---META---	NO	01/01/1970 05:30	01/01/1970 05:30	01/01/1970 05:30
□	\$LogFile		0 bytes	---META---	NO	01/01/1970 05:30	01/01/1970 05:30	01/01/1970 05:30
□	\$MFT		16384 bytes	---META---	NO	10/03/2023 10:03	10/03/2023 10:03	10/03/2023 10:03
□	\$MFTMirr		0 bytes	---META---	NO	01/01/1970 05:30	01/01/1970 05:30	01/01/1970 05:30
□	\$Secure		0 bytes	---META---	NO	10/03/2023 10:03	10/03/2023 10:03	10/03/2023 10:03
□	\$Secure\$SDS		266152 bytes	---ADS---	NO	10/03/2023 10:03	10/03/2023 10:03	10/03/2023 10:03
□	\$UpCase		0 bytes	---META---	NO	01/01/1970 05:30	01/01/1970 05:30	01/01/1970 05:30
□	\$UpCase\$Info		32 bytes	---ADS---	NO	01/01/1970 05:30	01/01/1970 05:30	01/01/1970 05:30
□	\$Volume		0 bytes	---META---	NO	01/01/1970 05:30	01/01/1970 05:30	01/01/1970 05:30

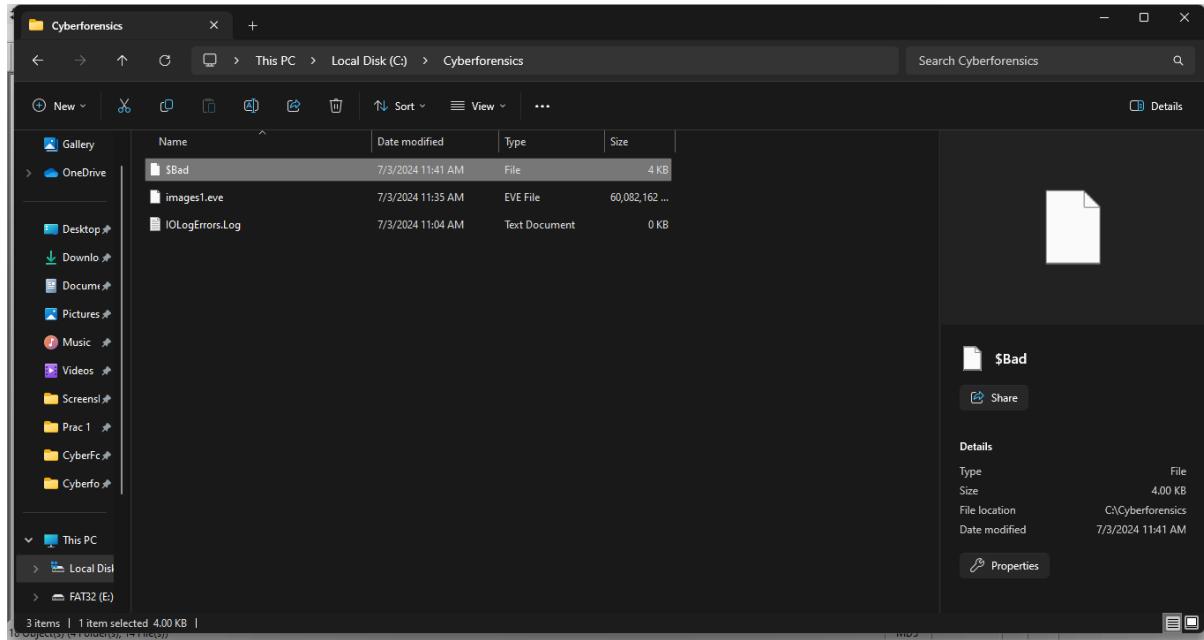
- Right click on deleted file, either view it or copy the file to a folder.



- Save the file



- Navigate to the folder and there you can see the deleted file.



- You can view the deleted file once saved in a folder.

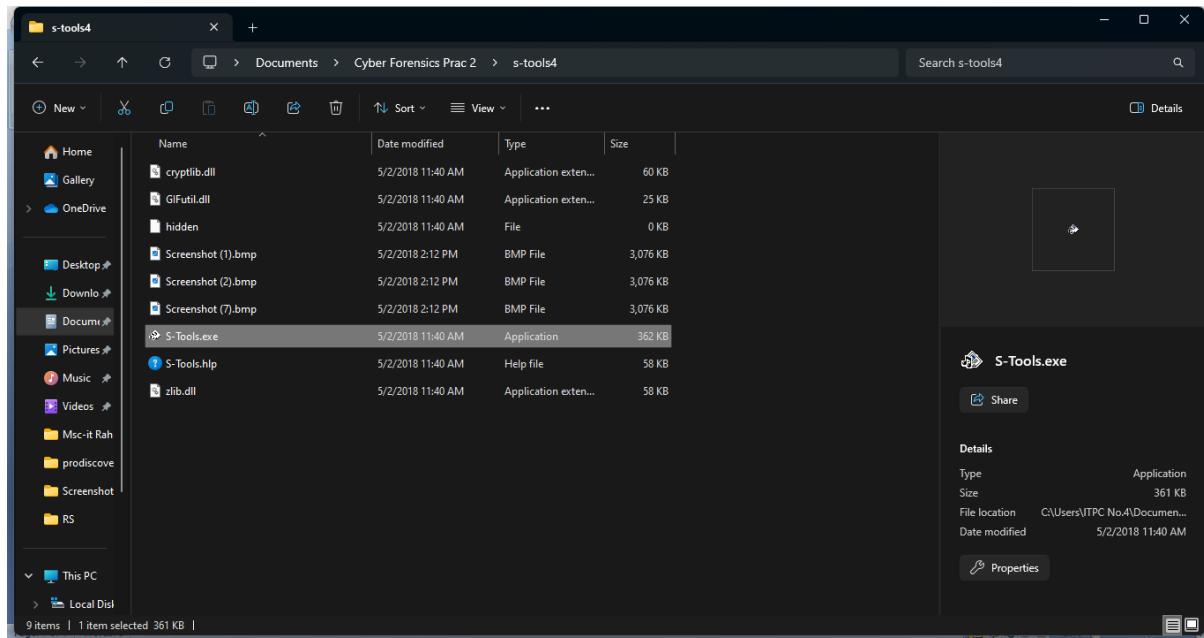
The screenshot shows a hex editor window with the file '\$Bad' open. The left pane displays the hex dump of the file, which consists mostly of zero bytes. The right pane shows the ASCII representation of the file, which includes some recognizable text like 'FILE0', 'H', 'D', 'MFT', 'H', 'D', 'FILE0', 'H', 'D', 'MFT', 'H', 'D', and 'Log File'. The word 'Bad' is highlighted in red in the ASCII view, indicating the deleted file's name.

Practical: 6

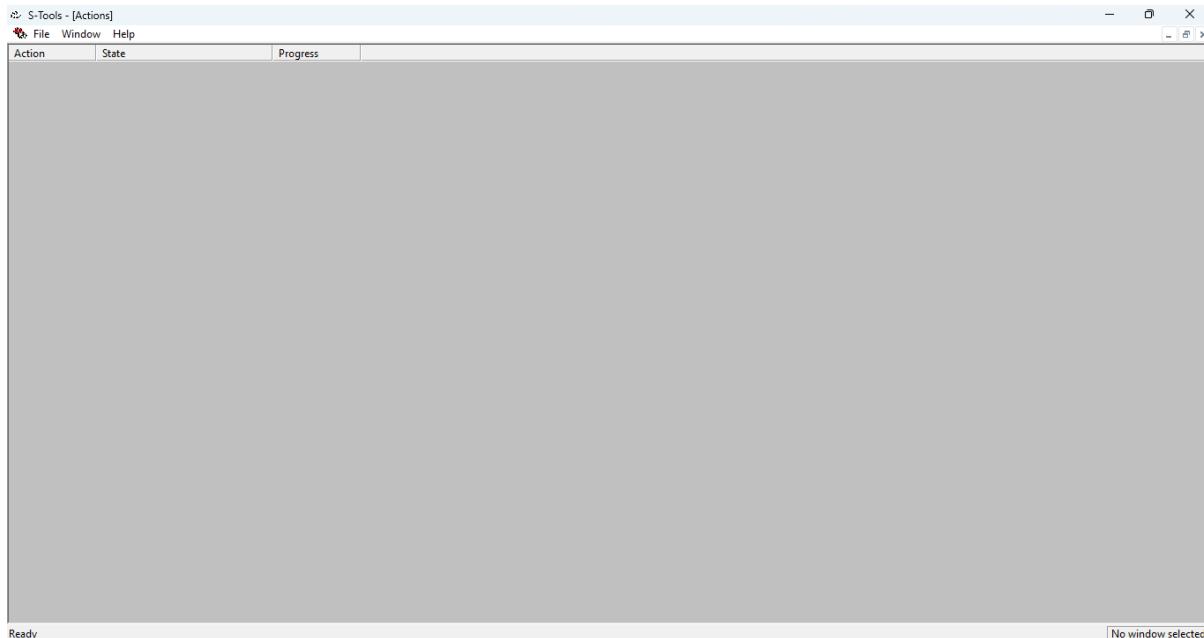
Aim: Using Steganography tools [S-Tools].

Writeup:

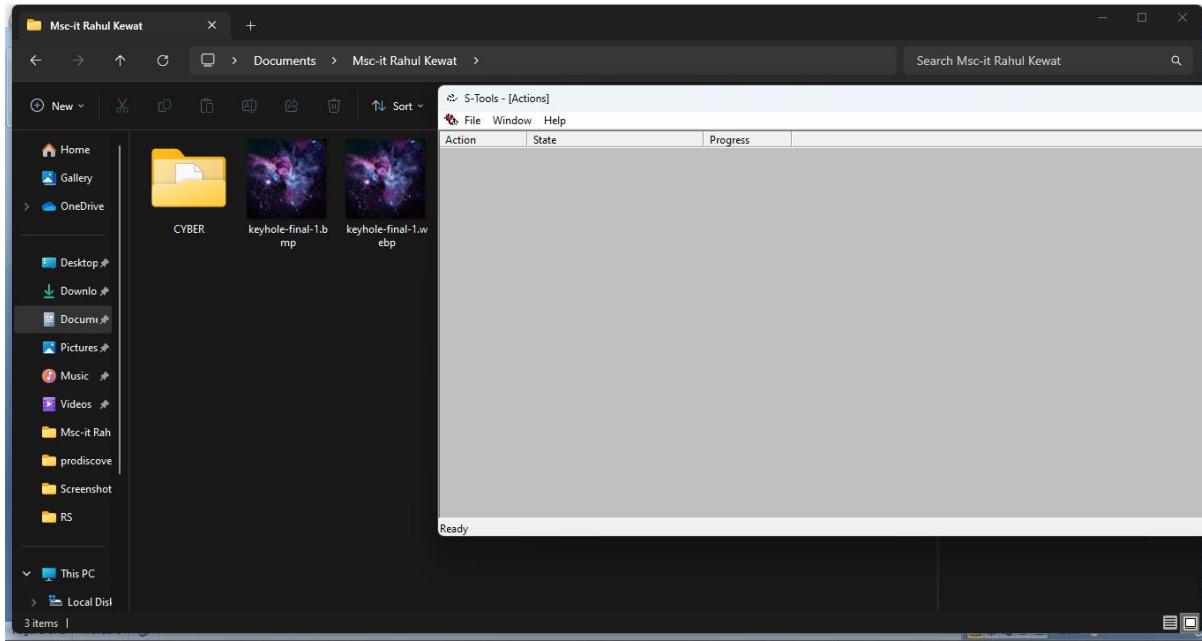
Step 1: Select the S-Tools.exe file and open the steganography software tool.



- S-Tools Window Open

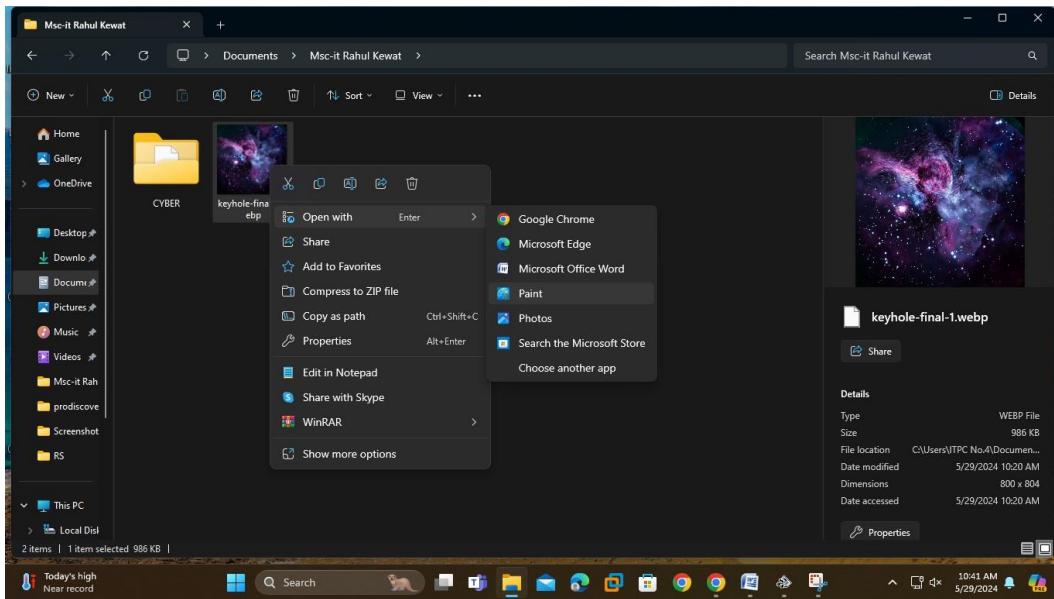


Step 2: With both the working directory and the S-Tools program open minimize both windows and place side-by-side. The S-Tools program is a drag and drop software. The files used to create the steganography file can be dragged from the directory into the S-Tools program.

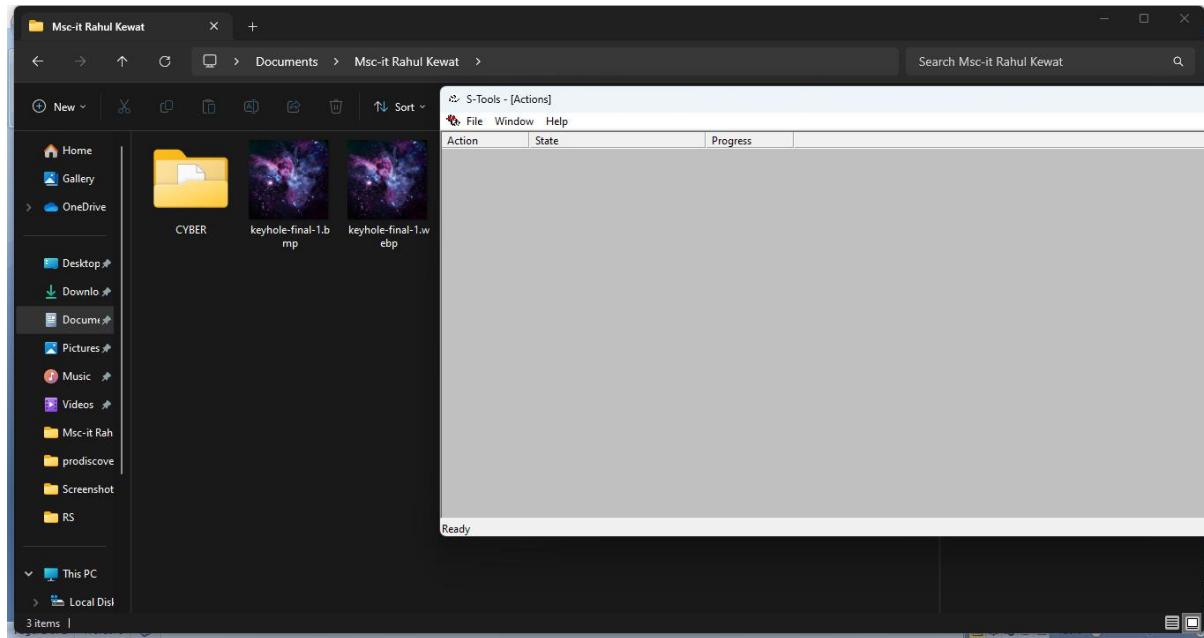


Step 3: If your image is in .jpg format, convert it to .bmp format by doing the following steps

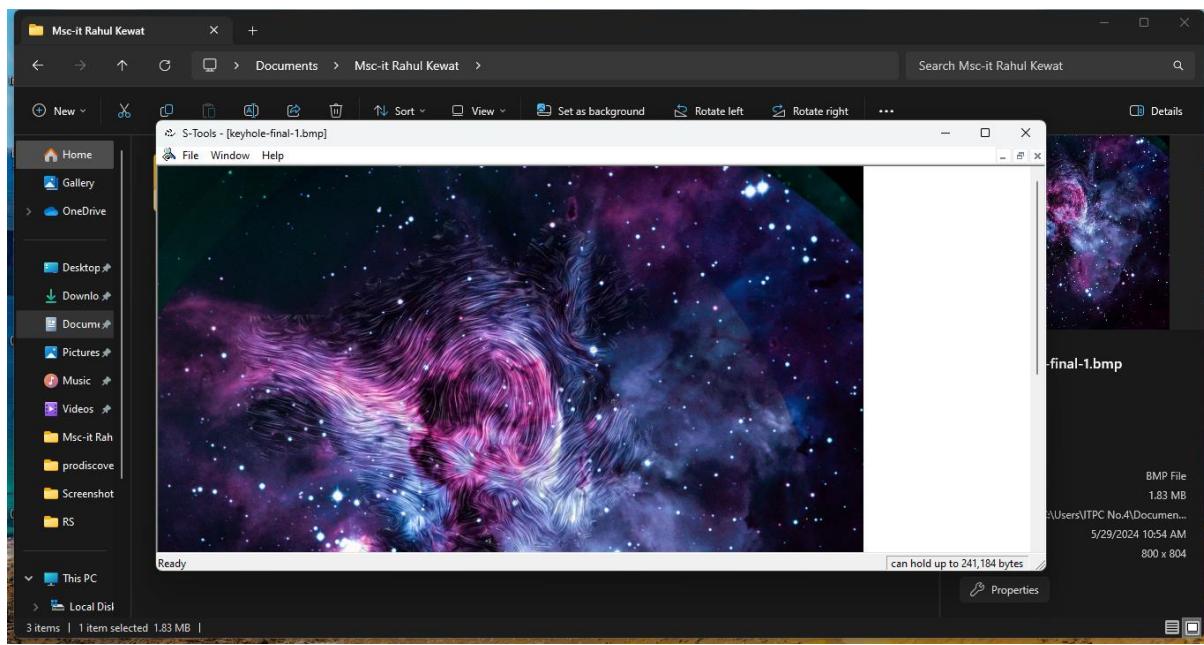
- Open the Selected Image With Paint and Save image in BMP format



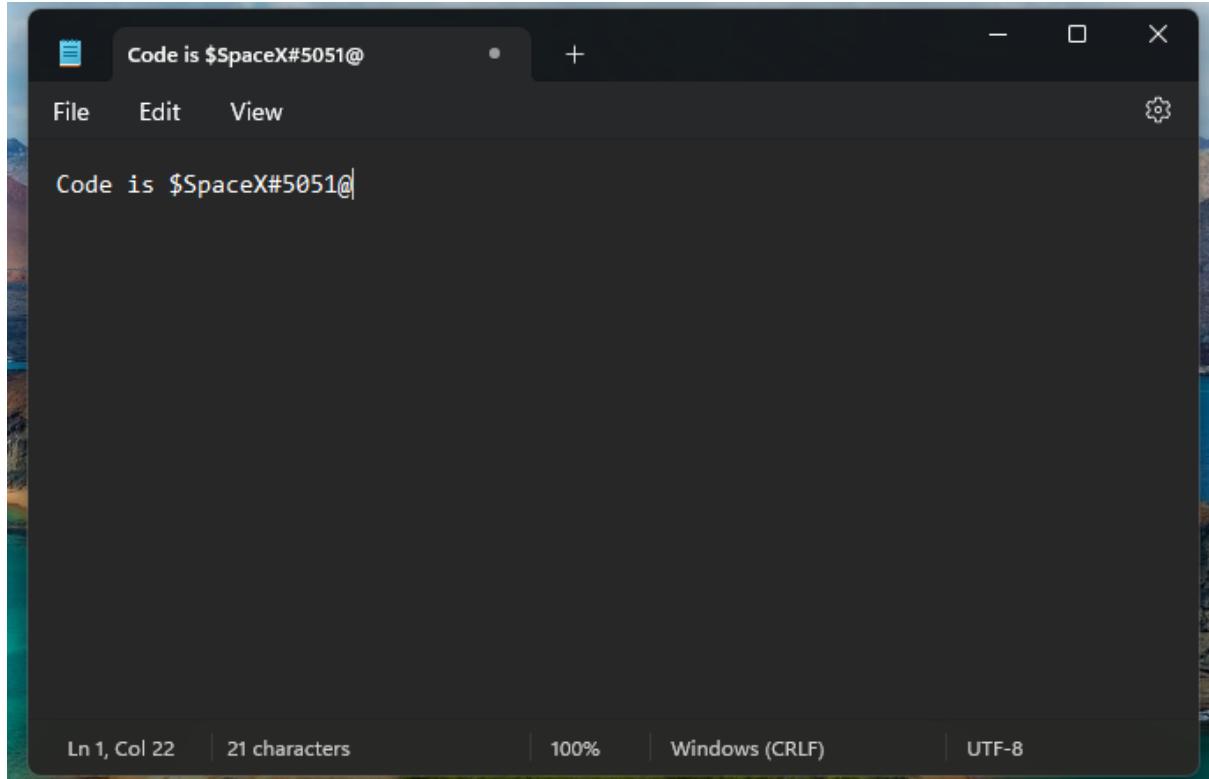
Step 4: The keyhole-final-1.bmp was selected and dragged onto the main window of the S-Tools program.



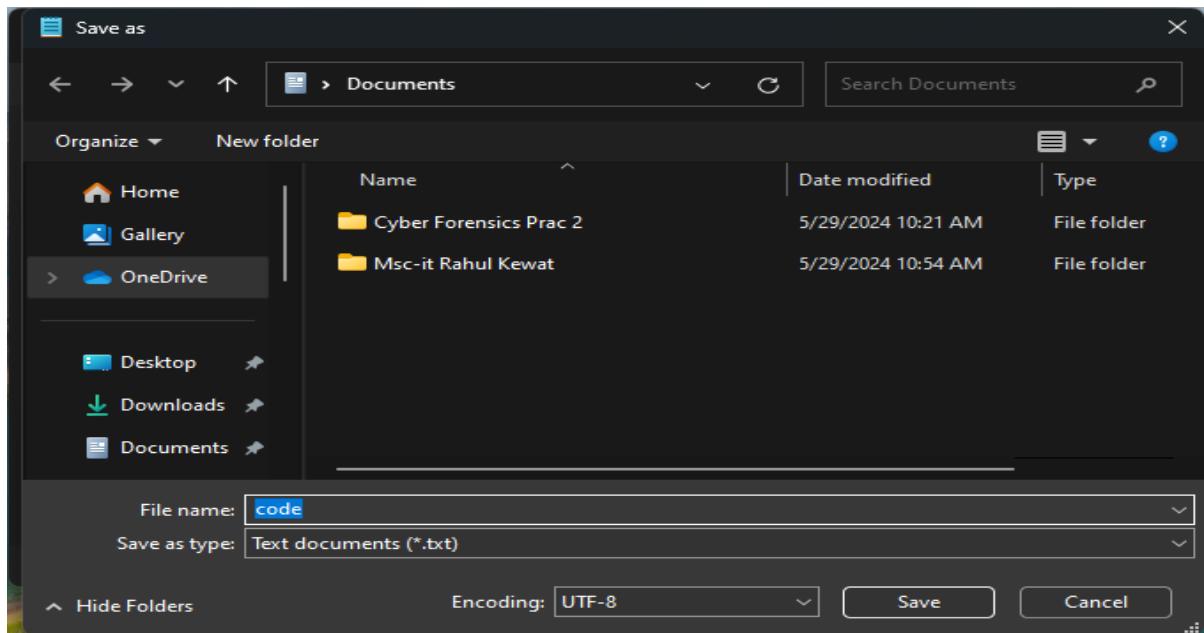
- The image is opened.



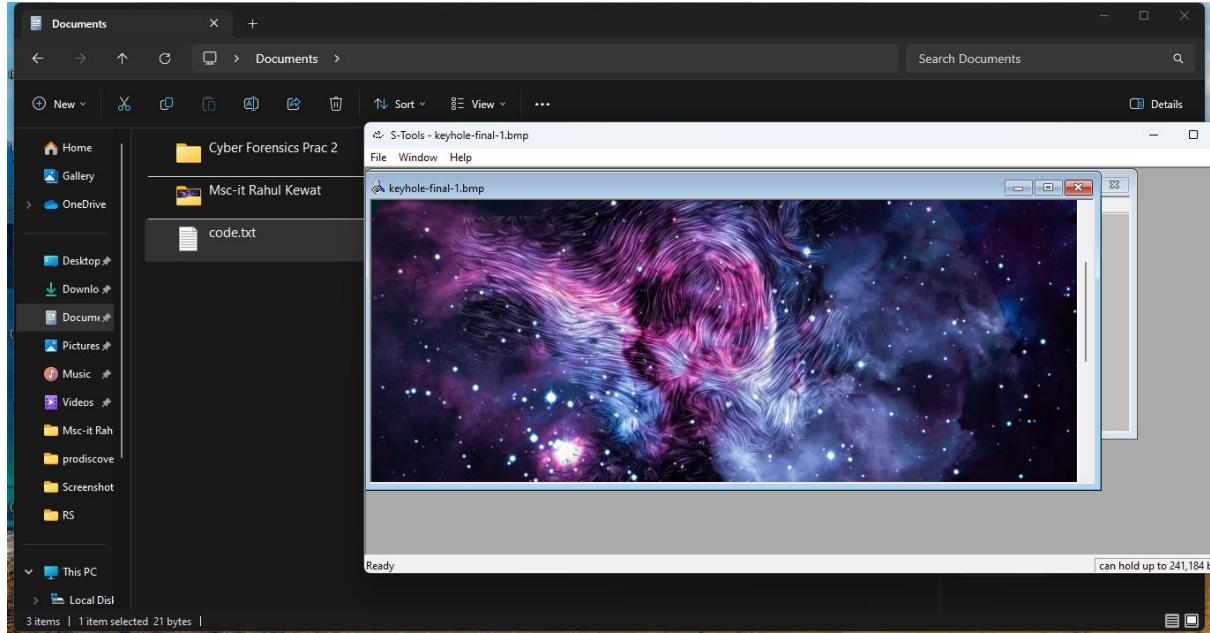
Step 5: Select a file to hide within the base file. If it's not there, create a txt.



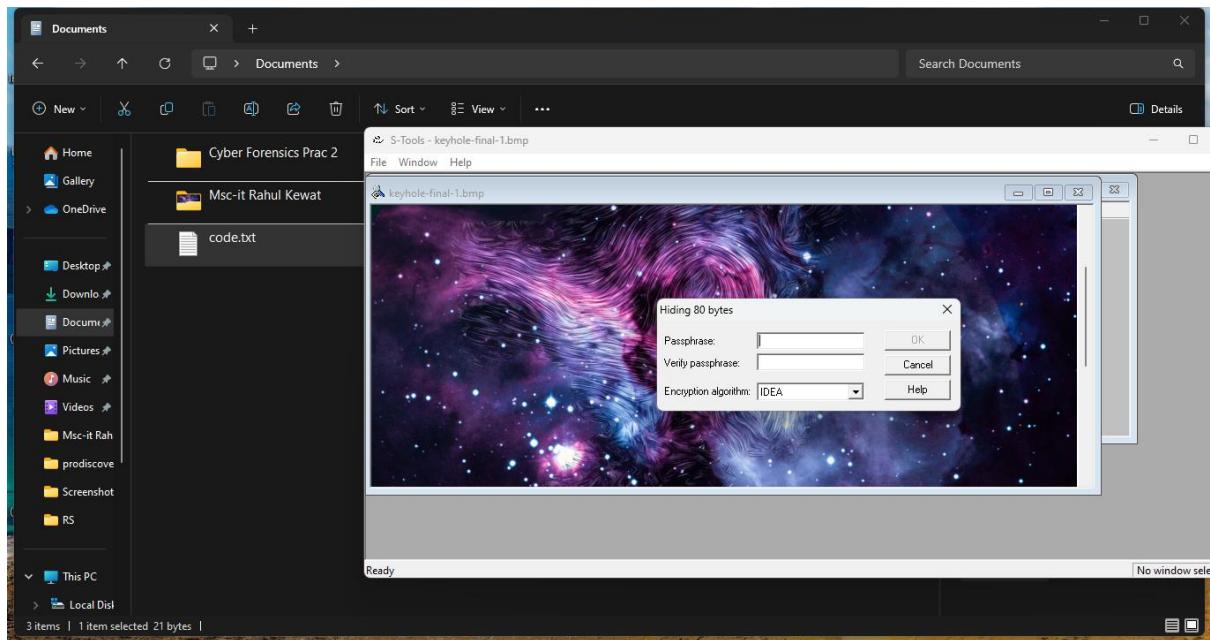
- **Save the file**



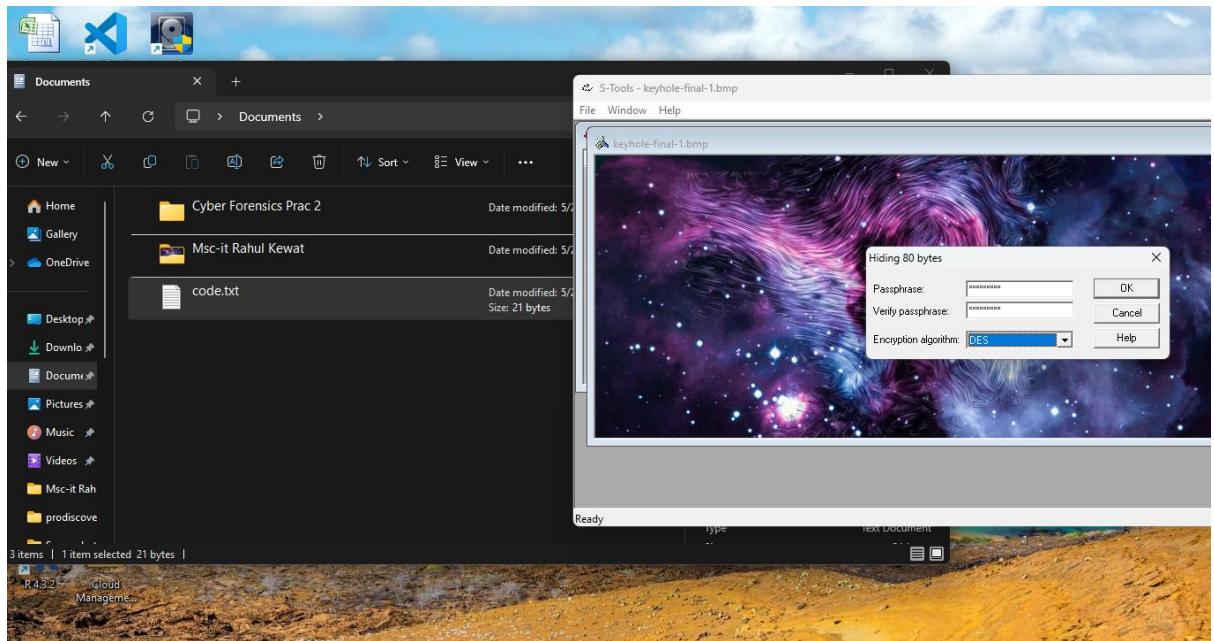
Step 5: The code.txt was selected and dragged onto the main window of the S-Tools program.



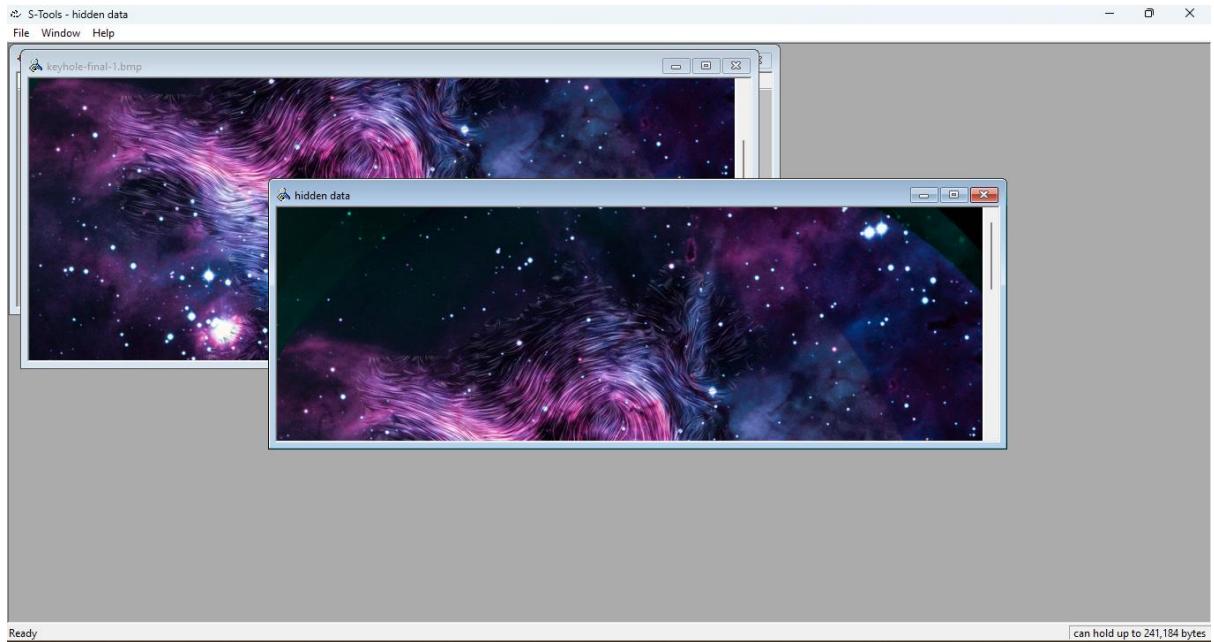
- After Dragged code.txt file onto main window of the S-Tools A dialogue box will appear asking the user to enter and verify a passphrase. Additionally, the user will have to select an encryption algorithm.



- Enter a **passphrase** in both the **passphrase** and **verify passphrase** text boxes. And **Click on OK**

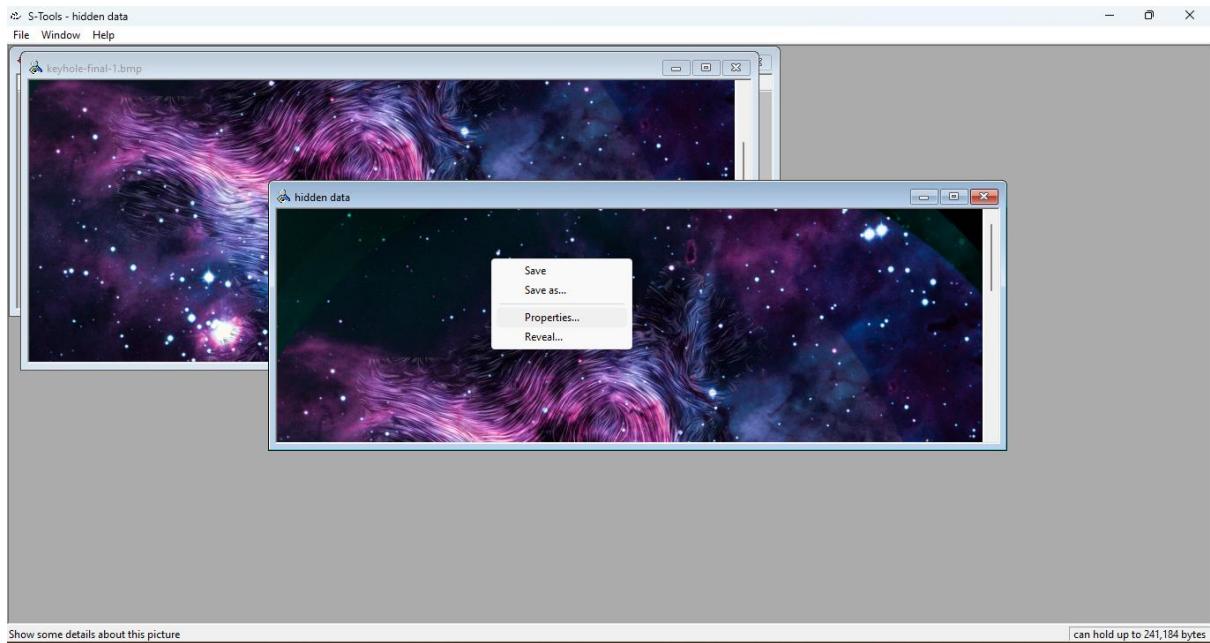


Step 6: The S-Tools main window will appear and a new file will be visible. The name of the file will be called **hidden data by default**.



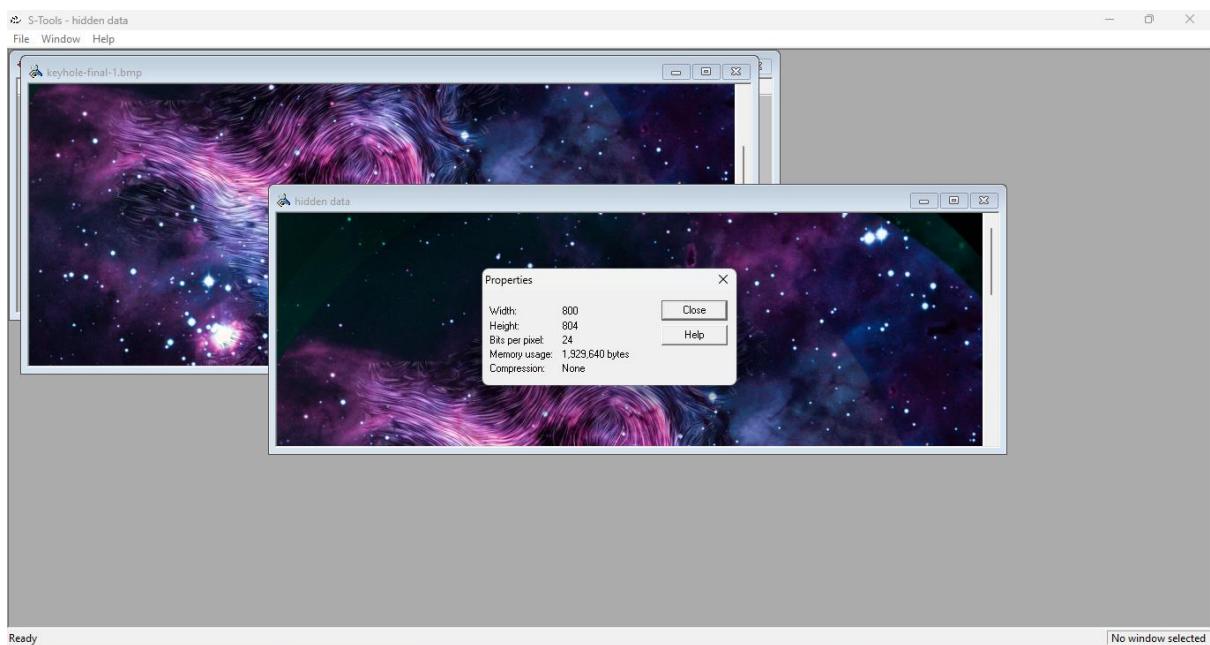
Step 7: Place the cursor on top of the hidden data image and select the right mouse button. The user will have four options available to them

- Save
- Save As
- Properties
- Reveal

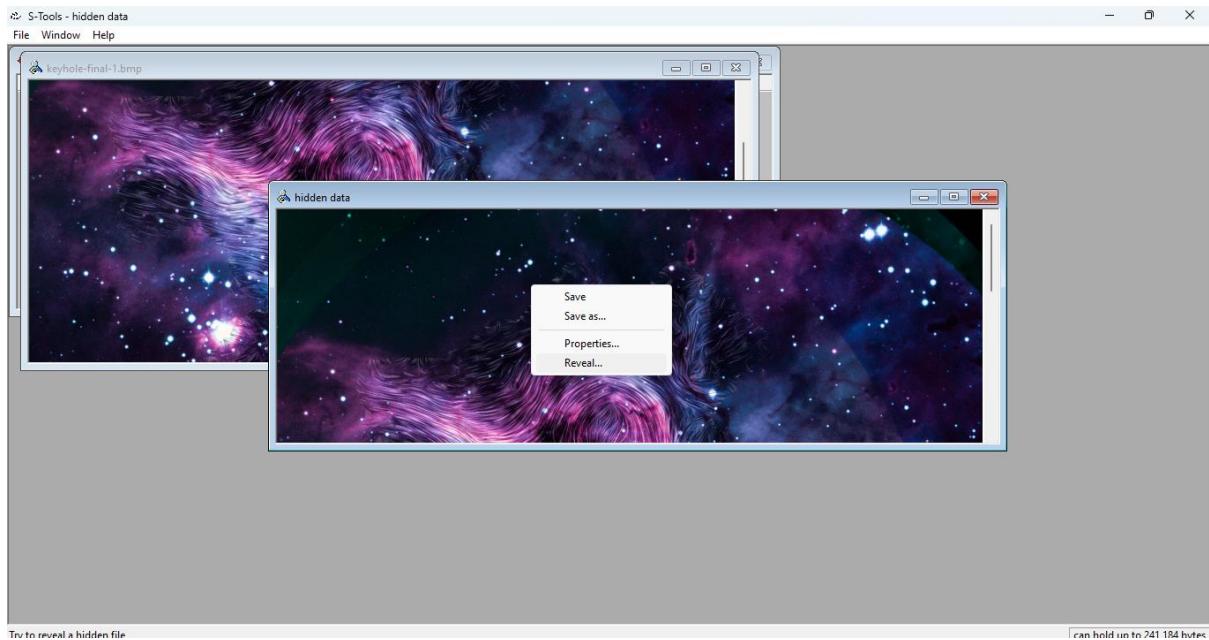


Step 8: Selecting the ‘Properties’ button while the cursor is over any image will display the following

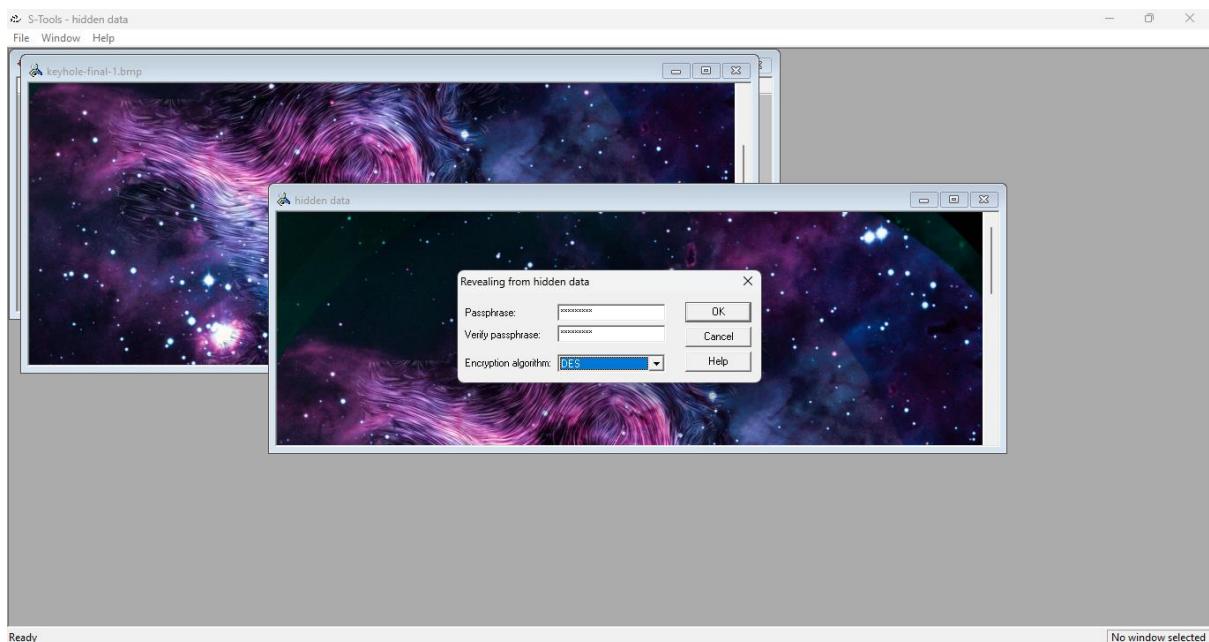
- Width and Height of the image
- Bits per pixel
- Memory Usage (file size in bytes)
- Compression



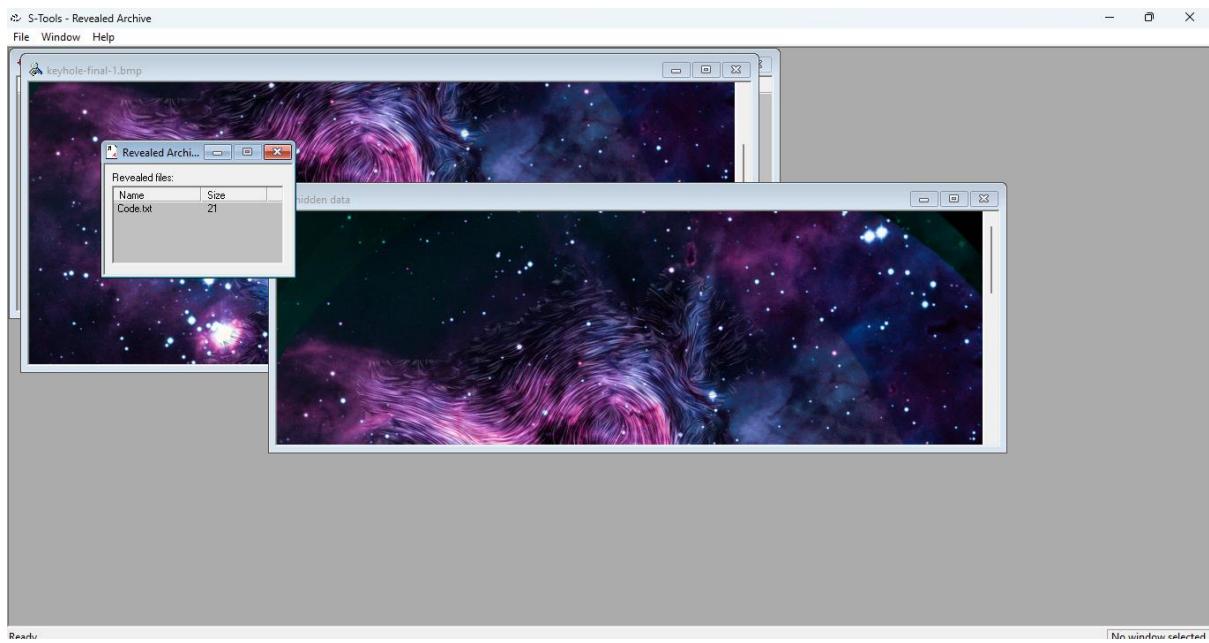
Step 9: Selecting the ‘Reveal’ button will display a passphrase dialogue box. A passphrase must be entered twice in the dialogue box and the correct encryption algorithm must be selected.



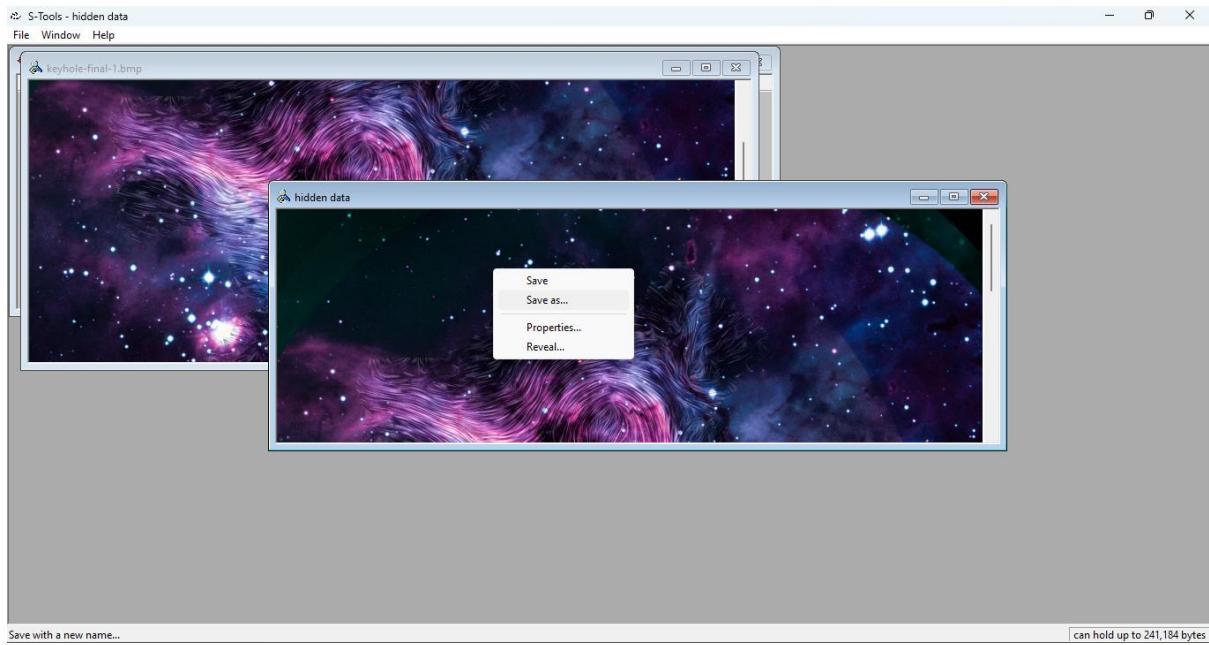
- Enter a passphrase twice, select the encryption algorithm, and **select the ‘OK’ button.**



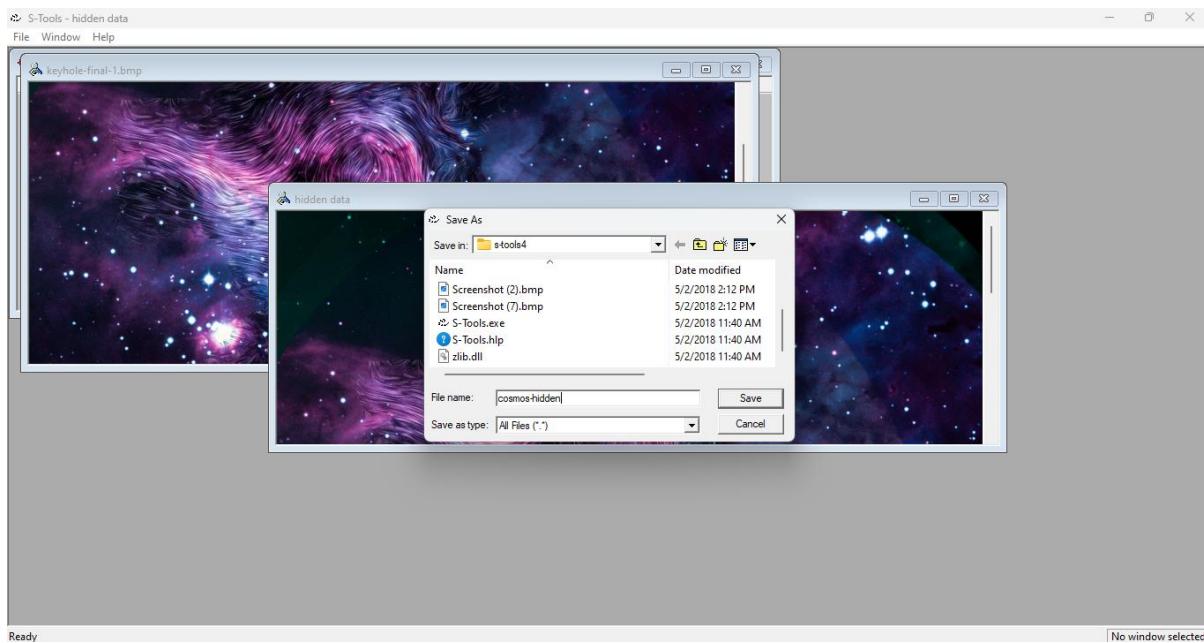
- A ‘Revealed Archive’ dialogue box will display which contains the file name and size of the hidden file.



Step 10: Select the Save as

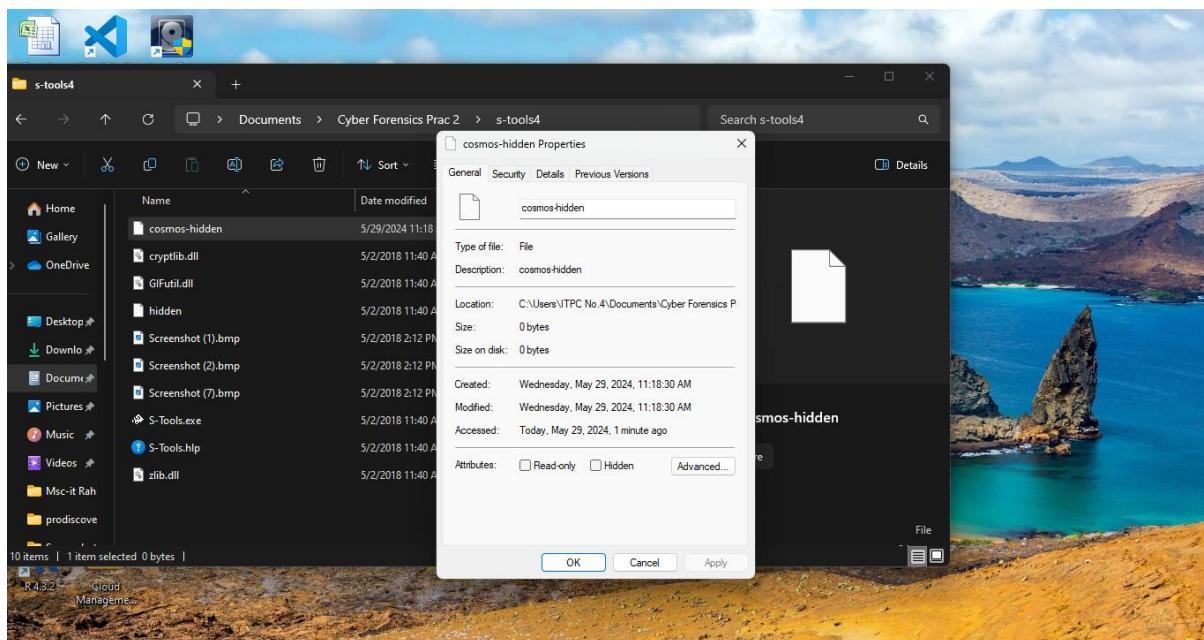


- A ‘Save As’ dialogue box will appear. Enter a valid file name, select the working directory and select the ‘Save’ button



Step 11: Locate the files in the working directory.

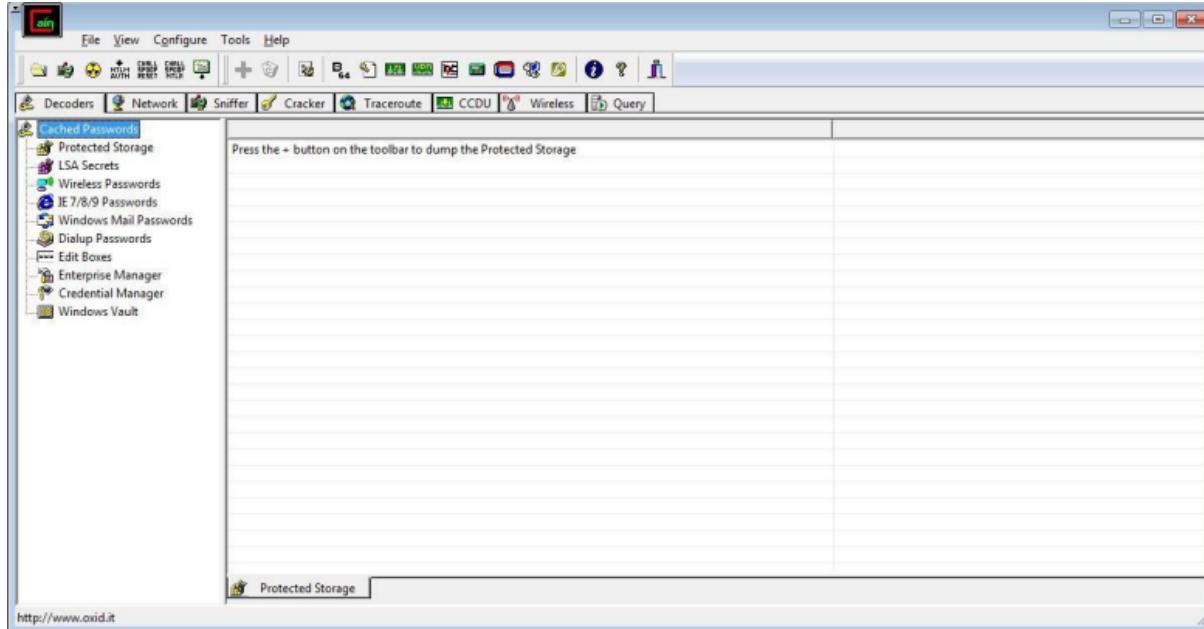
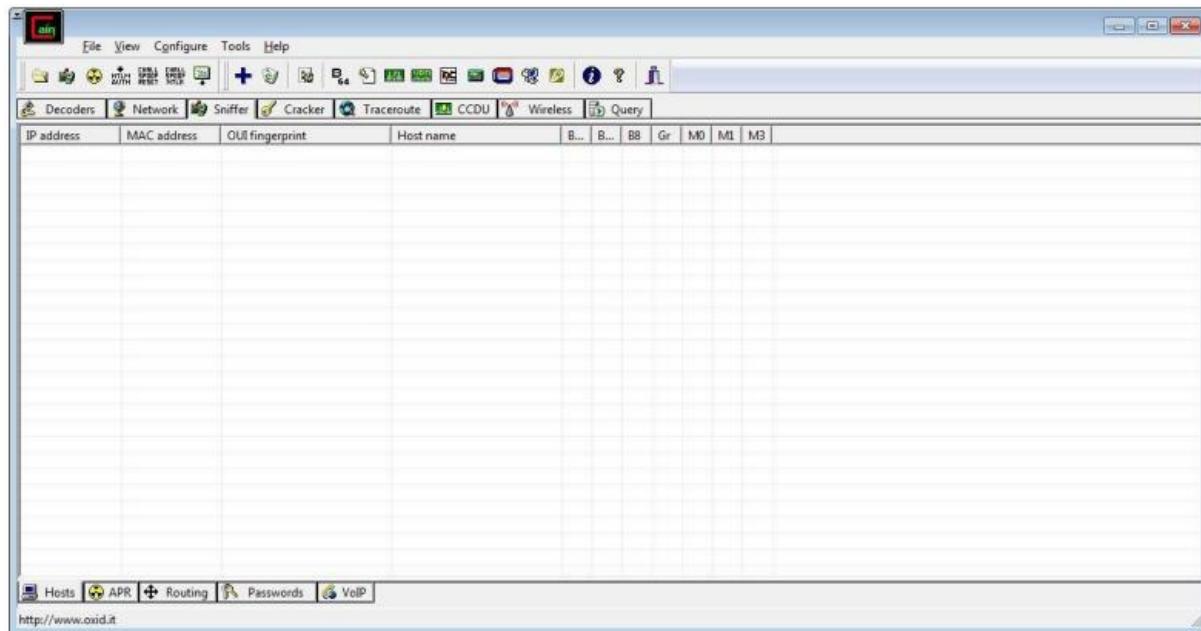
- Open the files using a multimedia software program and ensure that the files were extracted from the steganography file successfully.



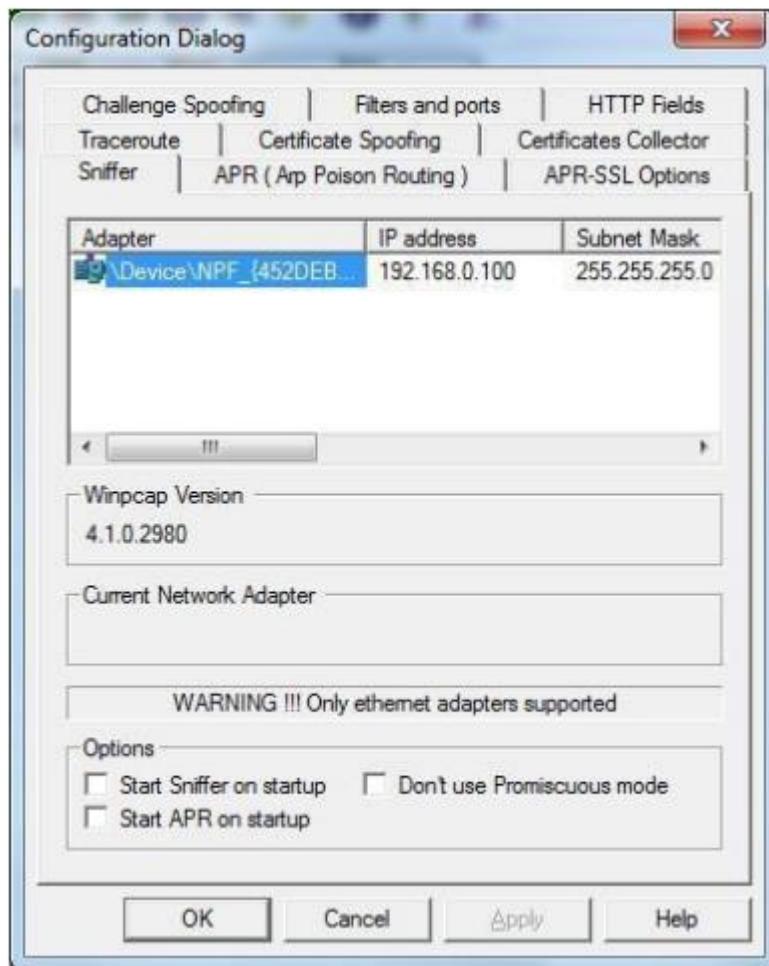
Practical: 7

Aim: Performing Sniffing and Password Cracking Using Cain and Abel.

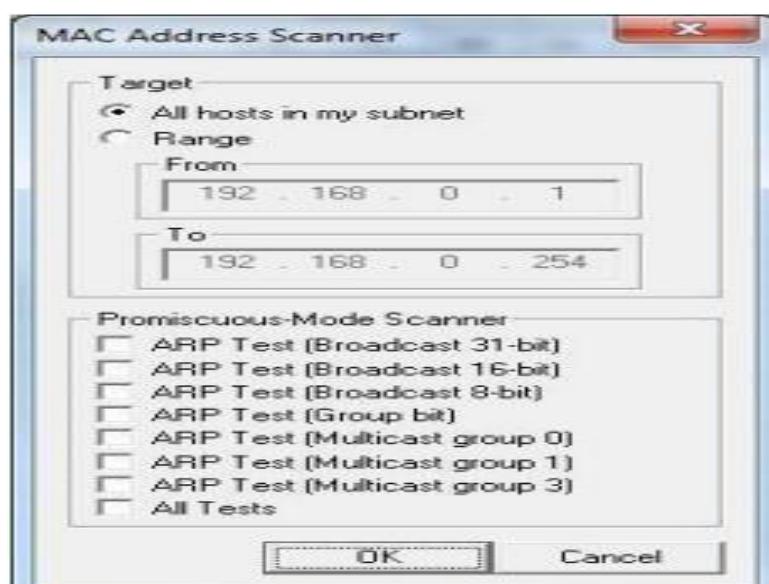
Writeup:

Step 1: Install and open Cain and Abel.**Step 2: Select sniffer on the top.**

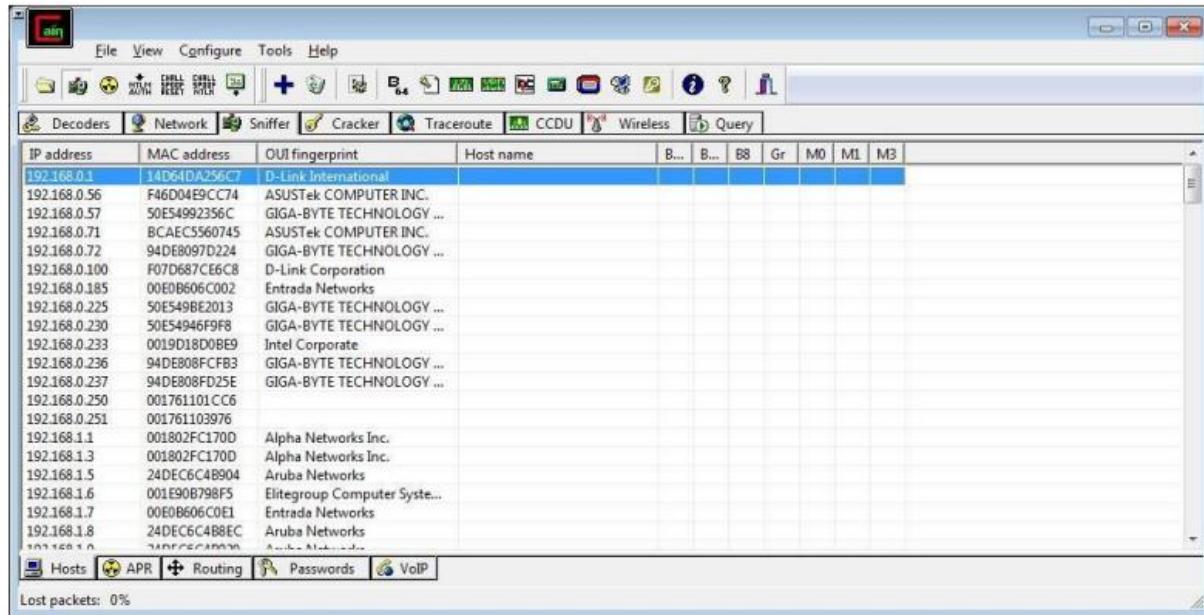
Step 3: Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



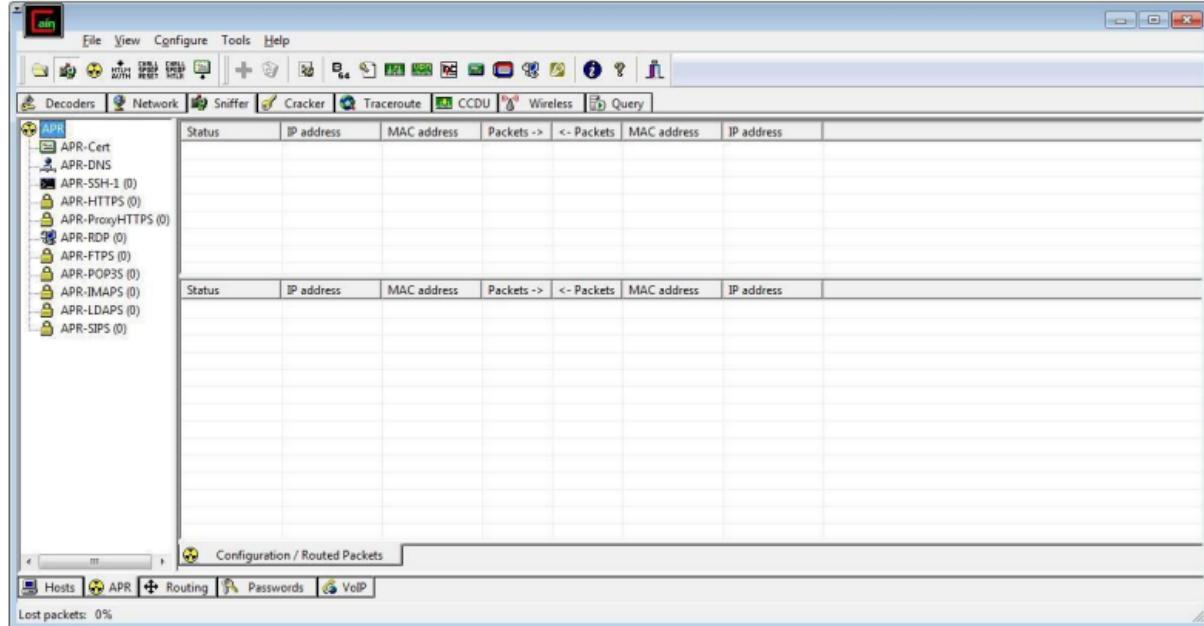
Step 4: Click on “+” icon on the top. Click on ok.



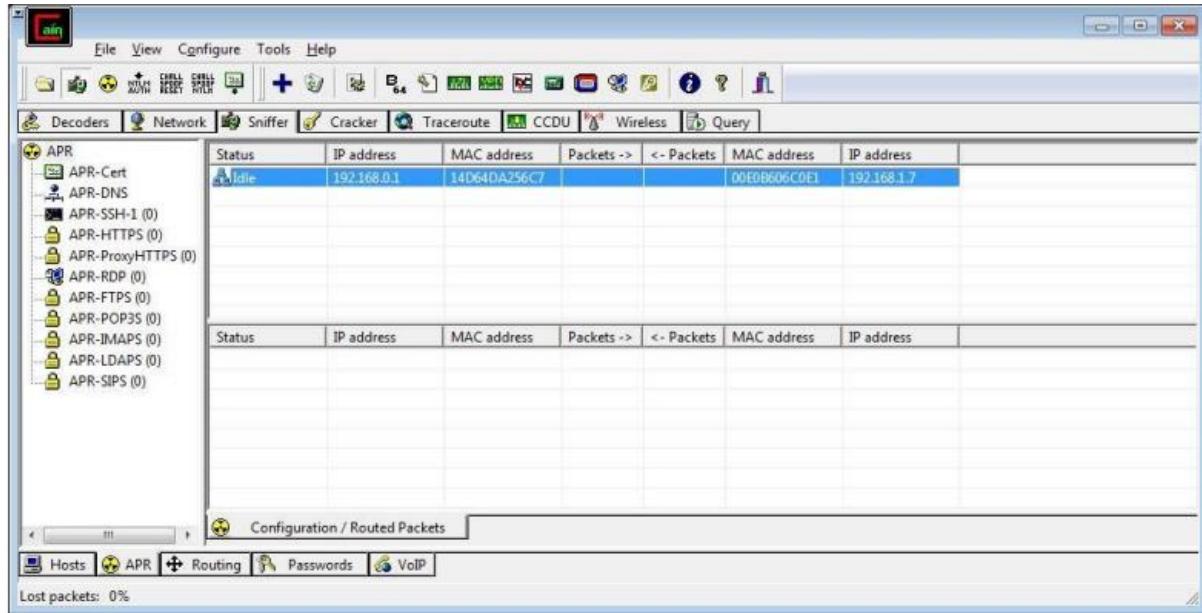
Step 5: Shows the Connected host.



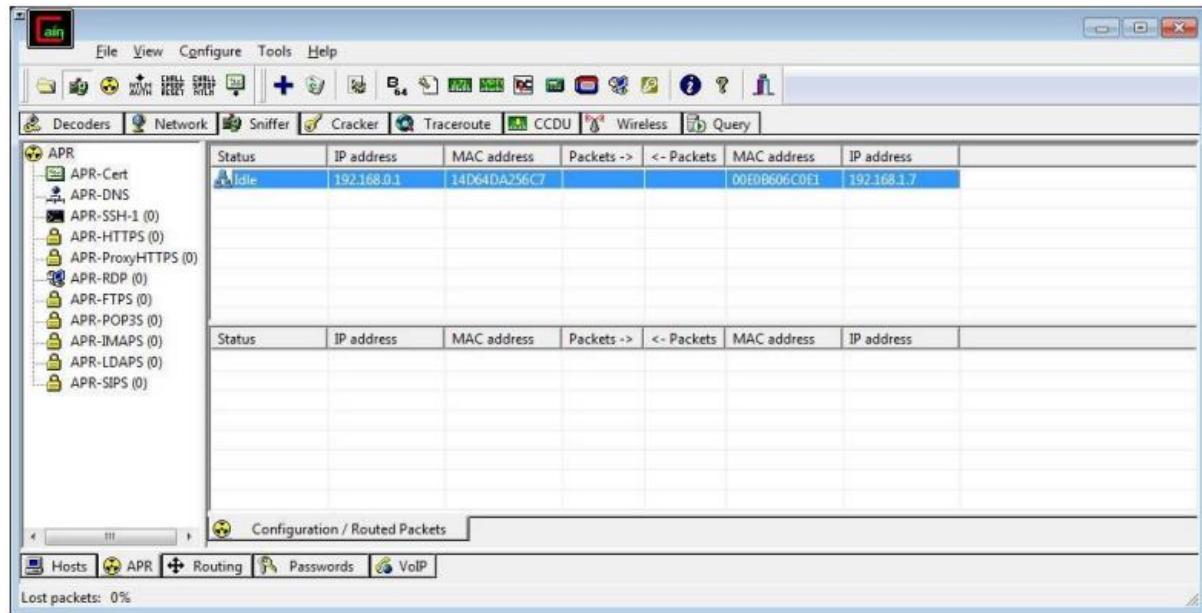
Step 6: Select Arp at bottom.



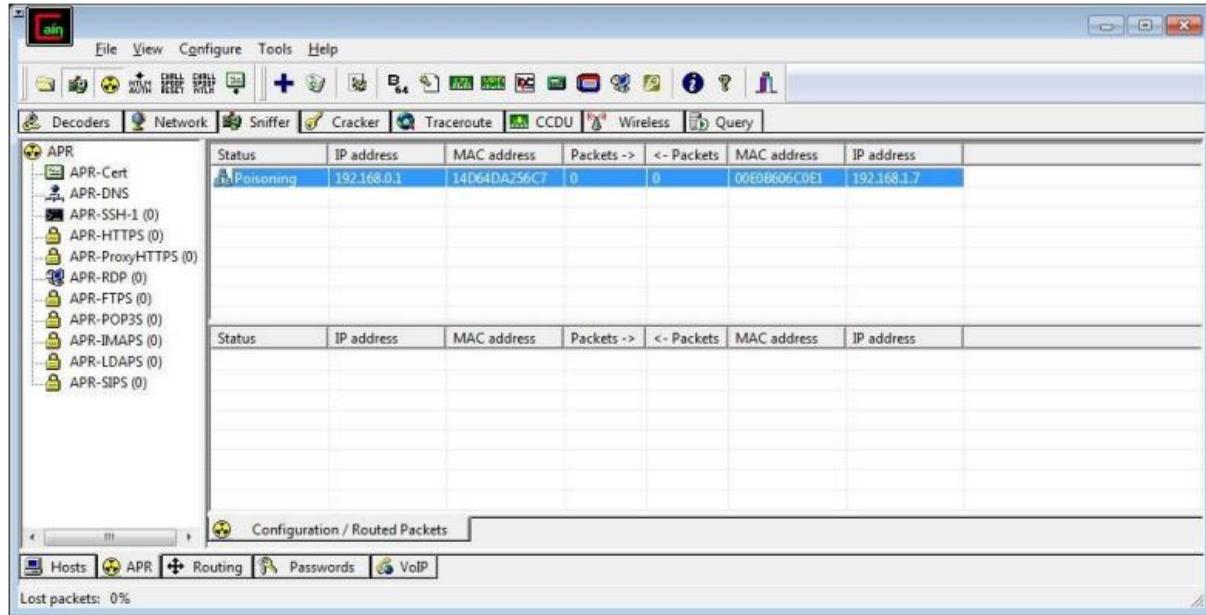
Step 7: Click on “+” icon at the top.



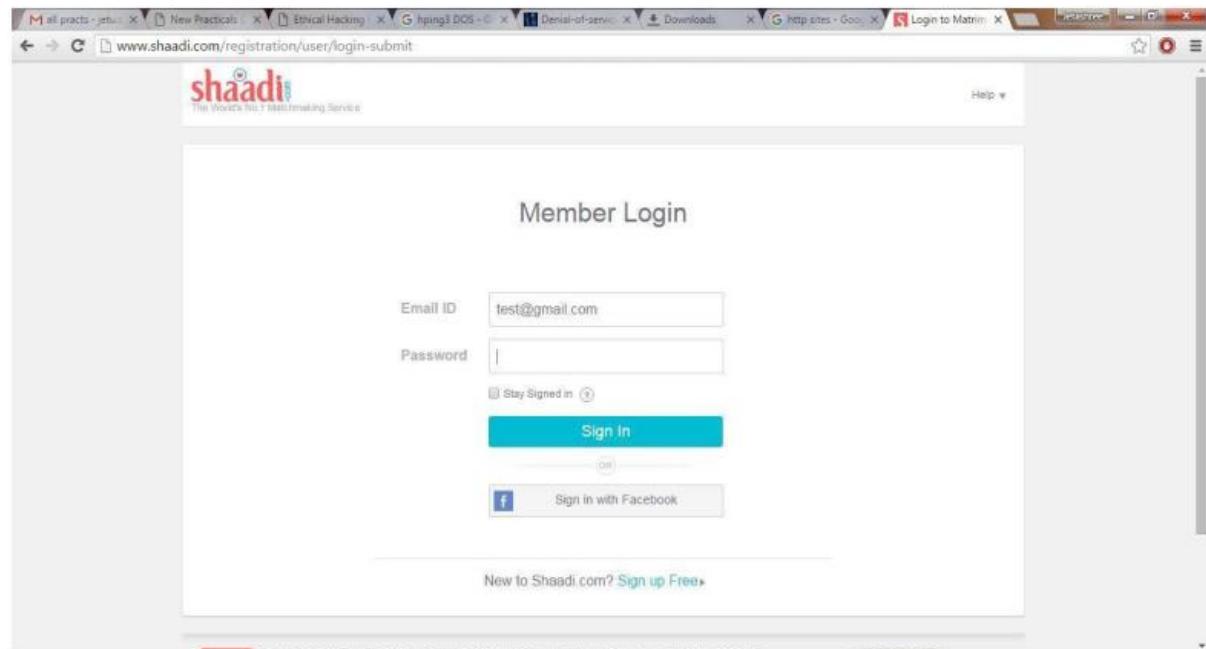
Step 8: Click on start/stop ARP icon on top.



Step 9: Poisoning the source.



Step 10: Go to any website on source ip address.



Step 11: Go to password option in the cain & abel and see the visited site password